Noname manuscript No.
(will be inserted by the editor)

Authentication schemes for Smart Mobile Devices: Threat Models, Countermeasures, and Open Research Issues

Mohamed Amine Ferrag[a,1], **Leandros Maglaras**[b,2,3], **Abdelouahid Derhab** [c,4], **Helge Janicke**[d,2]

[1]Department of Computer Science, Guelma University, 24000 Guelma, Algeria
[2]School of Computer Science and Informatics, De Montfort University, Leicester, UK
[3]General Secretariat of Digital Policy, Athens, Greece
[4]Center of Excellence in Information Assurance (CoEIA), King Saud University, Saudi Arabia

the date of receipt and acceptance should be inserted later

Abstract This paper presents a comprehensive investigation of authentication schemes for smart mobile devices. We start by providing an overview of existing survey articles published in the recent years that deal with security for mobile devices. Then, we give a classification of threat models in smart mobile devices in five categories, including, identity-based attacks, eavesdropping-based attacks, combined eavesdropping and identity-based attacks, manipulation-based attacks, and service-based attacks. This is followed by a description of multiple existing threat models. We also provide a classification of countermeasures into four types of categories, including, cryptographic functions, personal identification, classification algorithms, and channel characteristics. According to the characteristics of the countermeasure along with the authentication model iteself, we categorize the authentication schemes for smart mobile devices in four categories, namely, 1) biometric-based authentication schemes, 2) channel-based authentication schemes, 3) factors-based authentication schemes, and 4) ID-based authentication schemes. In addition, we provide a taxonomy and comparison of authentication schemes for smart mobile devices in form of tables. Finally, we identify open challenges and future research directions.

Keywords Security · Authentication · Smart Mobile Devices · Biometrics · Cryptography

1 Introduction

Mobile devices are going to take a central role in the Internet of Things era [1]. Smartphones, assisted with the 5G technology, that provides continuous and reliable connectivity [2], will soon be able to support applications across a wide variety of domains like homecare, healthcare, social networks, safety, environmental monitoring, e-commerce and transportation [3–5]. Storage capabilities of mobile phones increase rapidly, and phones can today generate and store large amounts of different types of data. Modern capabilities of smartphones such as mobile payment [6] and mobile digital signing of documents [7] can help the digitalization of both the private and the public sector, raising on the same time new security and privacy requirements [8–10].

As shown in Figure 1, there are two types of access to smart mobile devices during the authentication phase, namely, 1) users accessing smart mobile devices, and 2) users accessing remote servers via smart mobile devices. Mobile devices are protected with the use of different methods ranging from single personal identification numbers PINs, passwords or patterns which have been proved to be vulnerable to different kinds of attacks [11]. Moreover, it has been proven that the main breaches that systems face today, relate to attacks that can exploit human behavior, which call for more sophisticated security and privacy measures [12]. Even when strong authentication techniques are used during the initial access to the mobile device, there is a growing need for continuous authentication of legitimate users through users' physiological or behavioral characteristics [13]. In this way, approaches, which exploit biometrics, like fingerprint recognition, face recognition, iris recognition, retina recognition, hand recognition or even dynamic behavior such as voice recognition, gait patterns or even keystroke dynamics, can help detect imposters in real time [14]. Every new authentication method comes with a possible risk of low user acceptance due to latency and increasing complexity [15].

In order to secure stored data from falling into wrong hands, cryptographic algorithms, which are conventional methods of authenticating users and protecting communication messages in insecure networks, can be used [2]. Only the

[a]e-mail: ferrag.mohamedamine@univ-guelma.dz
[b]e-mail: leandros.maglaras@dmu.ac.uk
[c]e-mail: abderhab@ksu.edu.sa
[d]e-mail: heljanic@dmu.ac.uk

user who possesses the correct cryptographic key can access the encrypted content. Cryptographic algorithms can be categorized in two main groups [16], symmetric key cryptography and public key cryptography methods, where the latter although being more promising cannot be easily applied to short messages due to inducing big latency [17]. In the case that an adversary obtains the secret key of a legitimate user, this kind of attack is very difficult to be detected in the server side.

To conduct the literature review, we followed the same process used in our previous work [18]. Specifically, the identification of literature for analysis in this paper was based on specific keywords: "authentication scheme", "authentication protocol", "authentication system", and "authentication framework". By searching these keywords in academic databases such as SCOPUS, Web of Science, IEEE Xplore Digital Library, and ACM Digital Library, an initial set of relevant sources was located. Firstly, only proposed authentication schemes for smart mobile devices were collected. Secondly, each collected source was evaluated against the following criteria: 1) reputation, 2) relevance, 3) originality, 4) date of publication (between 2007 and 2018), and 5) most influential papers in the field. The final pool of papers consists of the most important papers in the field of mobile devices that focus on the authentication as their objective. Our search started on 01/11/2017 and continued until the submission date of this paper. The main contributions of this paper are:

- We discuss the existing surveys on security for smart mobile devices.
- We classify the threat models, which are considered by the authentication schemes in smart mobile devices, into five main categories, namely, identity-based attacks, eavesdropping-based attacks, combined eavesdropping and identity-based attacks, manipulation-based attacks, and service-based attacks.
- We review existing research on countermeasures and security analysis techniques in smart mobile devices.
- We provide a taxonomy and a side-by-side comparison, in a tabular form, of the state-of-the-art on the recent advancements towards secure and authentication schemes in smart mobile devices with respect to countermeasure model, specific mobile device, performance, limitations, computation complexity, and communication overhead.
- We highlight the open research challenges and discuss the possible future research directions in the field of authentication in smart mobile devices.

The remainder of this paper is organized as follows. Section 2 presents the existing surveys on security for mobile devices. In Section 3, we provide a classification for the threat models for mobile devices. In Section 4, we present countermeasures used by the authentication schemes for smart mobile devices. In Section 5, we present a side-by-side comparison in a tabular form for the current state-of-the-art of authentication schemes for mobile devices. Then, we discuss open issues and recommendations for further research in Section 6. Finally, we draw our conclusions in Section 7.

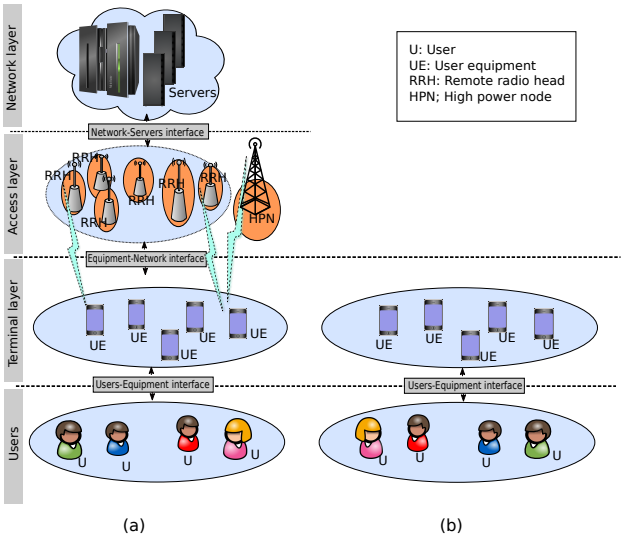

Fig. 1 Types of communication for the smart mobile devices during the authentication, (a) users accessing smart mobile devices, (b) users accessing remote servers via smart mobile devices

2 Existing Surveys on Security for Smart Mobile Devices

There are around ten survey articles published in the recent years that deal with security for mobile devices. These survey articles are categorized as shown in Table 1. La Polla et al. in [19] presented a survey on Security for Mobile Devices. They started by describing different types of mobile malware and tried to outline key differences between security solutions for smartphones and traditional PCs. They also presented the threats targeting smartphones by analyzing the different methodologies, which can be used to perform an attack in a mobile environment and explained how these methodologies can be exploited for different purposes. Based on their analysis, which was conducted back in 2013, the authors present security solutions, focusing mostly on those that use intrusion detection systems and trusted platform technologies. In the same year, Khan et al.in [3] performed a thorough survey on mobile devices, by considering them not as communication devices but as personal sensing platforms. Their research focused on two main categories, participatory and opportunistic mobile phone sensing systems. Having that in mind, they presented the existing work in the area of security of mobile phone sensing. They concluded that security and privacy issues need more attention while developing mobile phone sensing systems and appli-

Table 1 A summary of related survey papers

Ref.	Threat models	Countermeasures	Security analysis techniques	Security Systems	Authentication schemes	Surveyed papers
La Polla et al. (2013) [19]	√	√	X	√	0	2004 - 2011
Khan et al. (2013) [3]	X	X	X	√	X	2005 - 2008
Harris et al. (2014) [20]	X	X	X	√	X	2005 - 2012
Meng et al. (2015) [13]	0	√	X	0	0	2002 - 2014
Faruki et al. (2015) [21]	√	0	X	√	X	2010 - 2014
Teh et al. (2016) [22]	X	0	X	0	0	2012 - 2015
Alizadeh et al. (2016) [23]	0	0	X	0	0	2010 - 2014
Patel et al. (2016) [11]	0	X	X	0	0	2010 - 2015
Gandotra et al. (2017) [24]	√	0	X	√	X	2010 - 2015
Spreitzer et al. (2017) [25]	√	0	X	X	X	2010 - 2016
Kunda and Chishimba (2018) [26]	X	0	X	X	√	2010 - 2018
Our work	√	√	√	√	√	2007 - 2018

√ : fully; X: not; 0: partially supported

cations, since as mobile phones are used for social interactions, users' private data are vulnerable. Harris et al. [20] in their survey tried to identify all emerging security risks that mobile device imposes on SMEs and provided a set of minimum security recommendations that can be applied to mobile devices by the SMEs, based on the fundamental dilemma, whether to move to the mobile era, which results in facing higher risks and investing on costly security technologies, or postpone the business mobility strategy in order to protect enterprise and customer data and information.

Focusing on Android platforms, Faruki et al. in [21] surveyed several security aspects, such as code transformation methods, strength, and limitations of notable malware analysis and detection methodologies. By analyzing several malware and different methods used to tackle the wide variety of new malware, they concluded that a comprehensive evaluation framework incorporating robust static and dynamic methods may be the solution for this emerging problem.

Since password and PINs are authentication solutions with many drawbacks, Meng et al. in [13] conducted a thorough research on biometric-based methods for authentication on mobile phones. Authors included in their survey article both physiological and behavioral approaches, analyzed their feasibility of deployment on touch-enabled mobile phones and spotted attack points that exist and their corresponding countermeasures. Based on their analysis they concluded that a hybrid authentication mechanism that includes both multimodal biometric authentication along with traditional PINs or password can enhance both security and usability of the system. In order to further enhance security and privacy of mobile devices, active authentication techniques, which constantly monitor the behavior of the user, are deployed. These methods are surveyed in [11], where a thorough analysis of their advantages and limitations is presented along with open areas for further exploration. Using physiological and behavioral biometrics-based techniques similar to the ones surveyed in [13] on a continuous base and not only during initial access, multimodal biometrics-based fusion methods have been found to be the most efficient in terms of security and usability. One main issue that arises from the use of biometric characteristics is the possible theft of them, which can be prevented with the use of template protection schemes. A similar survey [22] that discusses touch dynamics authentication techniques for mobile devices was published in 2016. Touch dynamics belong to the category of behavioral biometrics and captures the way a person interacts with a touch screen device both for static and dynamic authentication of users. Teh et al. in [22] authors presented detailed implementations, experimental settings covering data acquisition, feature extraction, and decision-making techniques.

Alizadeh et al. in [23] discussed authentication issues in mobile cloud computing (MCC) and compare it with that of cloud computing. They presented both Cloud-side and user authentication methods and spotted those parameters that are important for designing modern authentication systems for MCC in terms of security, robustness, privacy, usability, efficiency, and adaptability. In another survey article that was published in 2017 [25], Spreitzer et al. focused on side-channel attacks against mobile devices and briefly discussed other attacks that have been applied mainly on smart cards or desktop/cloud settings, since the interconnectivity of these systems makes smartphones vulnerable to those attacks as well. Authors concluded that most of the attacks target Android devices, due to the big market share of Android platforms. They also recommended that future research should

focus on wearables, e.g. smart watches, that may suffer from the same attacks in the near future, and pointed out that side-channel attacks can be combined with other attacks that exploit software vulnerabilities in order to be more efficient.

Aslam et al. in [27] reviewed authentication protocols that are used on order to access the Telecare Medical Information Systems and discussed their strengths and weaknesses in terms of ensured security, privacy and computation cost. The schemes are divided into three broad categories of one-factor, two-factor, and three-factor authentication. Velasquez et al. in [28] presented existing authentication techniques and methods in order to discern the most effective ones for different contexts. In [29], Kilinc and Yanik reviewed and evaluated several SIP authentication and key agreement protocols according to their performance and security features. Finally in the last survey article, which was published in 2017 [24], Gandotra et al. surveyed device-to-device (D2D) communications along with security issues with the primary scope on jamming attacks. Finlayy, there is a special issue [30] for authentication on smart mobile devices that provides 20 papers range from many topics related to authentication techniques.

From the above survey articles, only five of them deal with authentication schemes for mobile devices and none of them thoroughly covers the authentication aspects that are related to mobile devices. To the best of our knowledge, this work is the first one that thoroughly covers the aspects of: threat models, countermeasures, security analysis techniques, security systems, and authentication schemes that were recently proposed by the research community.

3 Threat Models

In this section, we present and discuss the threat models that are considered by the authentication protocols in smart mobile devices. A summary of 26 attacks are classified into the following five main categories, according to the security property the attack trying to compromise: identity-based attacks (against authentication), eavesdropping-based attacks (against confidentiality), combined eavesdropping and identity-based attacks (against confidentiality and authentication), manipulation-based attacks (against integrity), and service-based attacks (against availability), as presented in Figure 2.

3.1 Identity-based attacks (against authentication)

The attacks under this category forge identities to masquerade as authorized users, in order to get access to the system. We classify 6 attacks, namely: Deposit-key attack, Impostor attack, Impersonation attack, Spoofing attack, Masquerade attack, and Replay attack.

- Deposit-key attack: It involves three parties: a roaming user, the user's home server, and the visiting foreign server of the roaming user. Under this attack, a malicious server makes the visiting foreign server believe that it is the user's home server. The roaming user deposits information at the visiting foreign server, which is also accessible by the user's fake home server (i.e., malicious server). In [31], this attack can be detected by verifying the key of foreign servers.
- Impostor attack: An adversary disables one of the co-located devices and attempts to impersonate it. To thwart this attack, the Diffie-Hellman key exchange is extended with a co-location verification stage to ensure that the pairing takes place between two co-located devices [32].
- Impersonation attack: An adversary tries to masquerade as a legitimate to log into the server. As presented in Figure 2, there are different authentication protocols [16, 33–43] that are resilient against this attack, and which use different ideas. The idea of chaotic hash-based fingerprint biometric is used in [33]. The idea of asymmetric encryption function is used by [34]. The idea of Elliptic curve cryptosystem is used in protocols [16, 35]. In addition, [36] uses bilinear pairings. [39] is based on an initial random seed number that is generated by the authorization authority. [40] and [41] adopt techniques based on Hashing functions and self-certified public keys respectively. The idea of mutual authentication is used in protocols [33, 38, 41]. [42] is based on Key-hash based fingerprint remote authentication scheme. Besides, pattern recognition approaches are adopted in [43]. [37] uses the idea of ransom values in which adversary cannot fabricate a fake request authentication message as he does not know the random value of a legitimate user and hence cannot masquerade as that user. On the other hand, the idea of mutual authentication is used in [38].
- Replay attack: It consists of spoofing the identities of two parties, intercepting data packets, and relaying them to their destinations without modification. As shown in Figure 2, there are 13 authentication protocols [16, 17, 31, 34, 35, 37, 39–42, 44–46] to deal with this attack. The idea of using signatures during the authentication phase is proposed in [34]. The idea of using different nonce variables in each login is adopted by protocols in [40, 41]. Protocols in [16, 17, 31, 35, 39, 44] use the idea of timestamps, which are combined with a randomly chosen secret key in protocols [45, 46]. Moreover, [37] proposes a one-way hashing function and random values, and [42] proposes random nonce and three-way challenge-response handshake technique.

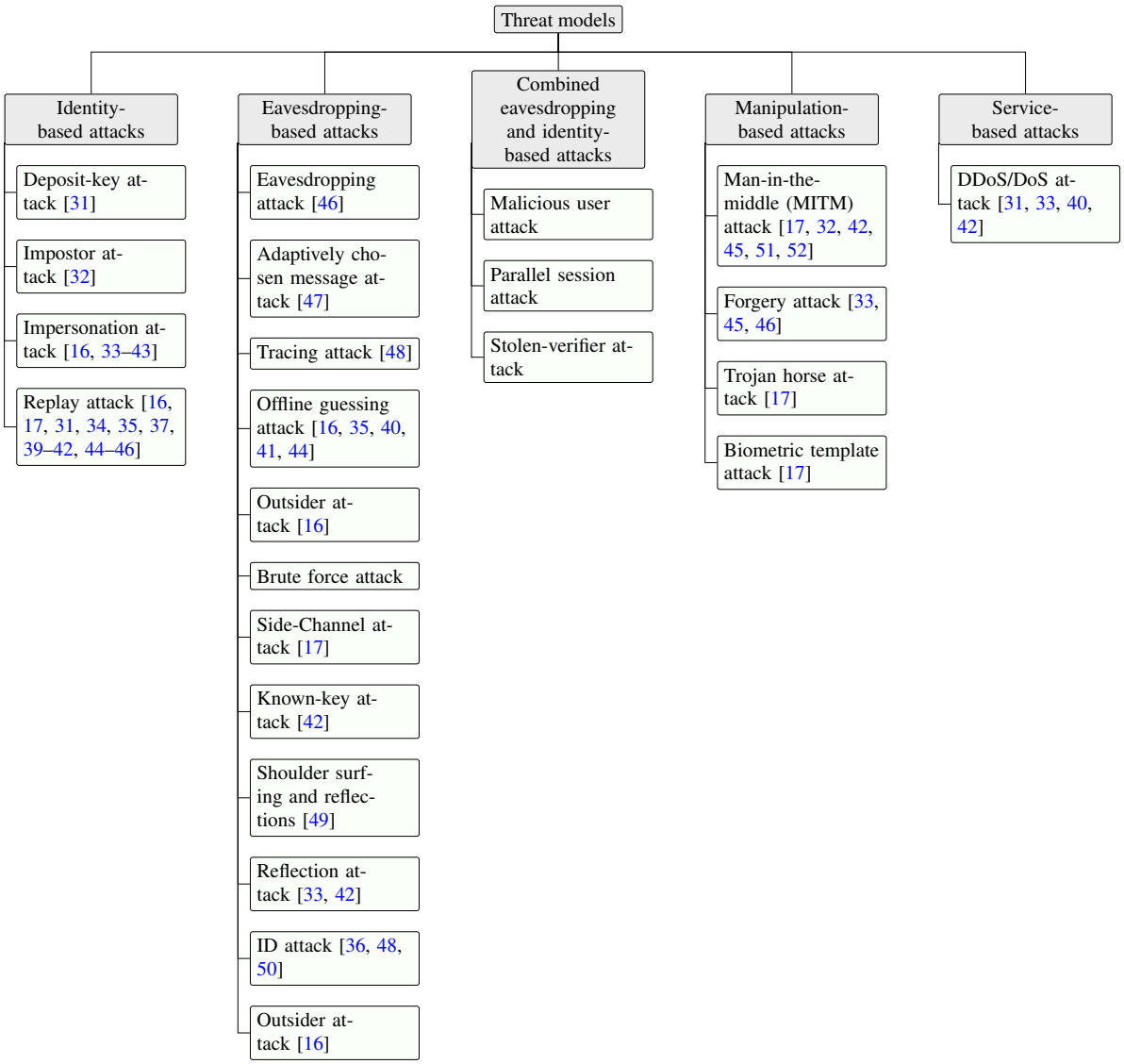

Fig. 2 Classification of threat models in smart mobile devices

3.2 Eavesdropping-based attacks (against confidentiality)

This category of attacks is based on eavesdropping the communication channel between the user and the server in order to get some secret information and compromise the confidentiality of the system. We can list the following attacks under this category:

- Eavesdropping attack: An attacker secretly overhears information that is transmitted over the communication channel, and which might not be authorized to know. The protocol in [34] deals with this attack by using a one-way hash function. On the other hand, the protocol in [46] uses encryption with the pairwise master key.
- Adaptively chosen message attack: Under this attack, an adversary attempts to forge a valid signature with the help of the private key generator (PKG). The objective of this attack is to gradually reveal information about an encrypted message or about the decryption key. To do so, ciphertexts are modified in specific ways to predict the decryption of that message. The protocol in [47] can resist against this attack as it uses a certificateless signature.
- Tracing attack: An adversary aims to collect enough privacy information to link data to a particular real identity. In order to resist against this attack, [48] uses random numbers in commitments and proofs.
- Offline guessing attack: An attacker collect useful information from an insecure channel or from a lost smart card. Then, the adversary guesses thousands of passwords per second and matches them with the captured one until the guessing operation succeeds. To thwart this attack, [41] employs the password salting mechanism, and pro-

tocols [16, 35, 40, 44] use the elliptic curve cryptosystem.
- Outsider attack: An adversary uses the overhead messages that are exchanged between user and server, in order to compute the secret key of the server. This attack is prevented in [16] by using the elliptic curve cryptosystem.
- Brute force attack: It consists of generating a large number of consecutive guessed passwords, with the hope of eventually guessing correctly. The resiliency against this attack is strengthened by employing cryptographic hash functions such as SHA-224.
- Side-Channel attack: It is based on information gained from the physical implementation of the cryptosystem. The physical electronic systems produce emissions about their internal process, which attackers gather in order to extract useful information. To resist against this attack, [17] proposes deploying elliptic curve cryptosystem as well as a Public Key Infrastructure (PKI).
- Known-key attack: It consists of compromising past session keys in order to derive any further session keys. In [42], the values that are used to compute the session keys are not available in plaintext. In addition, random nonce imparts dynamic nature to the session key, and hence the attacker cannot predict the value of the random nonce of the future session key.
- Shoulder surfing and reflections: It is a social engineering technique used to obtain information such passwords and other confidential data by looking over the victim's shoulder. To prevent this attack, [49] uses the idea of sightless two-factor authentication.
- Reflection attack: It is applicable to authentication schemes that adopt challenge-response technique for mutual authentication. Under this attack, a victim is tricked to provide the response to its own challenge. To deal with this attack, [33] proposes the chaotic hash-based fingerprint biometric remote user authentication scheme, and [42] proposes the key-hash based fingerprint remote authentication scheme.
- ID attack: An adversary sends some identities to obtain the private key of the corresponding identity. The security against this attack is ensured in [36, 48, 50] by using the idea of bilinear pairings.

3.3 Combined Eavesdropping and identity-based attacks

This category of attacks combines the eavesdropping and identity-based techniques to compromise the system. Under this category, we can find the following attacks:

- Malicious user attack: An attacker by extracting the credentials stored in a smart card, can easily derive the secret information of the system. After that, he masquerades as a legitimate user and accesses the system.
- Parallel session attack: This attack takes place under the assumption that multiple concurrent sessions are allowed between two communicating parties. An attacker that eavesdrops over an insecure channel and captures login authentication message from a user and the responding authentication message from the server, can create and send a new login message to the server, and masquerading as the user.
- Stolen-verifier attack: The attacker steals the verification data from the server of a current or past successful authentication session. Then, it uses the stolen data to generate authentication messages and send them to the server. If the server accepts the authentication messages, the adversary masquerades as a legitimate user.

3.4 Manipulation-based attacks (against integrity)

A data manipulation attack typically involves an unauthorized party accessing and changing your sensitive data, rather than simply stealing it or encrypting your data and holding it for ransom.

- Man-in-the-middle (MITM) attack: An attacker by spoofing the identities of two parties can secretly relay and even modify the communication between these parties, which believe they are communicating directly, but in fact, the whole conversation is under the control of the attacker. [42] proposes the key-hash based fingerprint remote authentication scheme to secure the system against this attack. In [32], Diffie-Hellman key exchange with a co-location verification stage is proposed. [45] combines bilinear pairing and elliptic curve cryptography. On the other hand, [17] uses the idea of combining biometric fingerprint and the ECC public key cryptography, whereas symmetric encryption and message authentication code are used in [51]. The Multi factors-based authentication scheme is adopted in [52].
- Forgery attack: An attacker forges valid authentication messages to satisfy the requirement of the authentication scheme. To resist against this attack, [33] proposes the chaotic hash-based fingerprint biometric remote user authentication scheme. On the other hand, [45, 46] uses the idea of pairing and elliptic curve cryptography.
- Trojan horse attack: It uses a Trojan horse program to compromise the authentication system. In order to prevent the Trojan horse program from tampering the biometric authentication module, [17] integrates biometric and cryptography.
- Biometric template attack: An adversary attacks the biometric template in the database to add, modify, and delete templates in order to gain illegitimate access to the sys-

tem. To increase the security strength of the biometric template, [17] maximizes its randomness.

3.5 Service-based attacks (against availability)

The goal of service-based, or Denial of Service (DoS) attacks, is to make the authentication service unavailable either by (1) flooding the authentication server with huge amount of data to make it busy and unable of providing service to the legitimate users, or (2) updating the verification information of a legitimate user with false data. Afterwards, a legitimate legal user is unable to login to the server. As depicted in Figure 2, there are four authentication protocols [31, 33, 40, 42] to prevent or detect DoS attacks. In [33], the user has to perform authentication by using a biometric fingerprint. If the mobile device is stolen or lost, illegitimate users cannot make a new password, and hence [33] is resistant against the denial-of-service attack. As for protocol in [31], it is only required that the user and the foreign server to be involved in each run of the protocol, and the home server can be off-line. Consequently, DoS attack on home servers is not possible. On the other hand, [40] uses the idea of one-way hash function, and [42] proposes a key-hash based fingerprint remote authentication scheme.

4 Countermeasures and security analysis techniques

A secure and efficient authentication scheme is needed to prevent various insider and outsider attacks on many different smart mobile devices. The authentication scheme uses both cryptosystems and non-cryptosystem countermeasures to perform the user authentication whenever a user accesses the devices. In this section, we will discuss the countermeasures and security analysis techniques used by the authentication schemes for smart mobile devices.

4.1 Countermeasures

The countermeasures used by the authentication schemes for smart mobile devices can be classified into four categories, including, cryptographic functions, personal identification, classification algorithms, and channel characteristics, as presented in Figure 3. Table 2 presents the countermeasures used in authentication schemes for smart mobile devices.

4.1.1 Cryptographic functions

Cryptographic functions are used in most authentication schemes for smart mobile devices in order to achieve several security goals, and can be classified into three types of categories, including, asymmetric encryption function, symmetric encryption function and, hash function. As presented in Table 2, two cryptographic functions are the most used, namely, 1) Bilinear pairings and 2) Elliptic curve cryptosystem (ECC). The authentication schemes [16], [35], [45], [44], [17], [78], [79] use the elliptic curve cryptosystem [29] to reduce the computation loads for mobile devices but they still suffer from some disadvantages such as the need for a key authentication center to maintain the certificates for users' public keys. Using ECC, the scheme in [16] provides mutual authentication and supports a session key agreement between the user and the server. The scheme in [45] employs ECC and pairing to manipulate authentication parameters and authorization keys for the multiple requests in mobile pay-TV systems. The scheme in [44] uses ECC with three-way challenge-response handshake technique in order to provide the agreement of session key and the leaked key revocation capability. Note that hash functions are used specifically to preserve the data integrity. In this subsection, we will briefly introduce the bilinear pairings and the elliptic curve cryptosystem.

Bilinear pairings Le G_1 and G_2 be multiplicative groups of the same prime order p, respectively. Let g denote a random generator of $G_1$and $e : G_1 \times G_1 \rightarrow G_2$ denote a bilinear map constructed by modified Weil or Tate pairing with following properties:

- Bilinear: $e\left(g^a, g^b\right) = e(g,g)^{ab}$, $\forall g \in G_1$ and $\forall a,\ b \in Z_p^*$. In particular, $Z_p^* = \{x | 1 \leq x \leq p-1\}$.
- Non-degenerate: $\exists g \in G_1$ such that $e(g,g) \neq 1$.
- Computable: there exists an efficient algorithm to compute $e(g,g)$, $\forall g \in G_1$.

Elliptic curve cryptosystem As discussed by Guo et al. [48], the bilinear pairing operations are performed on elliptic curves. An elliptic curve is a cubic equation of the form $y^2 + axy + by = x^3 + cx^2 + dx + e$, where a, b, c, d, and e are real numbers. In an elliptic curve cryptosystem (ECC) [29], the elliptic curve equation is defined as the form of $E_p(a,b)$: $y^2 = x^3 + ax + b (\text{mod } p)$ over a prime finite field F, where $a,\ b \in F_p$, $p > 3$, and $4a^3 + 27b^2 \neq 0 \ (\text{mod } p)$. Given an integer $s \in F_p^*$ and a point $P \in E_p(a,b)$, the point multiplication $s \cdot P$ over $E_p(a,b)$ can be defined as $s \cdot P = P + P + \cdots + P$ (s *times*). Generally, the security of ECC relies on the difficulties of the following problems [16]:

Definition 1. Given two points P and Q over $E_p(a,b)$, the elliptic curve discrete logarithm problem (ECDLP) is to find an integer $s \in F_p^*$ such that $Q = s \cdot P$.

Definition 2. Given three points P, $s \cdot P$, and $t \cdot P$ over $E_p(a,b)$ for $s,\ t \in F_p^*$, the computational Diffie-Hellman problem (CDLP) is to find the point $(s \cdot P) \cdot P$ over $E_p(a,b)$.

Table 2 Countermeasures used by the authentication schemes for smart mobile devices

Countermeasure	Scheme
Personal Identification Number (PIN)	[53] [54] [55] [52]
Ear Shape	[56]
Electrocardiogram	[57] [58]
Capacitive touchscreen	[59]
Behaviour profiling	[60]
Linguistic profiling	[60]
Gait recognition	[61]
Rhythm	[62] [63]
Touch dynamics	[64] [49]
Multi-touch interfaces	[65] [66]
Probabilistic polynomial time algorithms	[31]
Initial random seed number	[39]
A unique international mobile equipment identification number	[39]
Encryption with pairwise master key	[46]
Identity-based elliptic curve algorithm	[46]
Tag number	[34]
Keystroke analysis	[53] [54] [67] [68] [55] [69] [60] [70]
Diffie-Hellman key exchange	[32]
Classification algorithms	[54] [71] [38] [72] [73]
Chaotic hash	[33]
Fingerprint	[33] [17] [40] [42] [74]
Teeth image	[71]
Voice recognition	[71] [55] [52]
HMM biosensor scheduling	[75]
Asymmetric encryption function	[34]
Symmetric encryption function	[34] [38] [39] [51]
Hash function	[34] [33] [45] [37] [50] [38] [39] [44] [17] [76] [41] [42] [77] [78] [79]
Elliptic curve cryptosystem	[16] [35] [45] [44] [17] [78] [79]
Bilinear pairings	[36] [45] [50] [76] [41] [48] [77]
Password	[37] [38] [68] [51] [52]
Schnorr's signature scheme	[76]
Self-certified public keys	[41]
Graphical password	[80]
Message authentication code	[51]
Channel characteristics	[81]
Face recognition	[82] [52] [73]
Iris recognition	[82] [43]
Certificateless signature	[47]
Homomorphic encryption	[48] [83]
Order preserving encryption	[83]
Gaze gestures	[84]
Arm gesture	[56]
Signature recognition	[85]

Definition 3. Given two points P and $Q = s \cdot P + t \cdot P$ over $E_p(a,b)$ for s, $t \in F_p^*$, the elliptic curve factorization problem (ECFP) is to find two points $s \cdot P$ and $t \cdot P$ over $E_p(a,b)$.

4.1.2 Personal identification

As shown in Figure 4, the personal identification can be classified into two types of categories, including:

Numbers-based countermeasures (e.g, Personal Identification Number (PIN), International Mobile Equipment Identity (IMEI), and Password). Using the inter-keystroke latency, the Clarke and Furnell's scheme [53] classifies the users based upon entering telephone numbers and PINs, where the users are authenticated based upon three interaction scenarios: 1) Entry of 11-digit telephone numbers, 2) Entry of 4-digit PINs, and 3) Entry of text messages. Similar to the scheme [53], Clarke and Furnell's framework collects the following input data types, 1) Telephone numbers, 2) Telephone area code (5-Digit), 3) Text message, and 4) 4-Digit PIN code. According to Wiedenbeck et al. [86], the numbers-based countermeasures should be easy to remember; they should be random and hard to guess; they should

Table 3 Security analysis techniques used by the authentication schemes for smart mobile devices

Ref.	Time	Tool	Authentication model	Main results
[54]	2007	- Pattern recognition approaches	- User authentication	- Evaluating the feasibility of utilizing keystroke information in classifying users
[71]	2008	- Pattern recognition approaches	- User authentication	- Evaluating the feasibility of utilizing together teeth image and voice
[36]	2009	- Random oracle model - Computational assumptions	- Mutual authentication	- Show that the proposed protocol is secure against ID attack
[45]	2009	- Computational assumptions	- Hand-off authentication - Anonymous authentication	- Show that the proposed scheme can protecting identity privacy
[50]	2010	- Random oracle model - Computational assumptions	- Mutual authentication	- Show that an adversary should not know the previous session keys
[64]	2012	- Pattern recognition approaches	- User authentication	- Evaluating the feasibility of touch dynamics
[65]	2012	- Pattern recognition approaches	- User authentication	- Show that the multi-touch gestures great promise as an authentication mechanism
[66]	2012	- Pattern recognition approaches	- Continuous mobile authentication	- Evaluating the applicability of using multi-touch gesture inputs for implicit and continuous user identification
[76]	2012	- Computational assumptions	- Mutual authentication with key agreement	- Construct an algorithm to solve the CDH problem or the k-CAA problem
[72]	2013	- Pattern recognition approaches	- Continuous authentication	- Feasibility of continuous touch-based authentication
[51]	2013	- Formal proof - Random oracle model	- Transitive authentication	- Solving the CDH problem
[47]	2014	- Game theory	- Anonymous authentication	- Prove that the authentication scheme achieves anonymity, unlinkability, immunity of key-escrow, and mutual authentication
[43]	2016	- Pattern recognition approaches	- Multimodal authentication	- Show that the sensor pattern noise-based technique can be reliably applied on smartphones
[46]	2017	- Pattern recognition approaches	- Active authentication	- Show the performance of each individual classifier and its contribution to the fused global decision

be changed frequently, and should be different for different user's accounts; they should not be written down or stored in plain text. Therefore, the numbers-based countermeasures are vulnerable to various types of attacks such as shoulder surfing.

Biometrics-based countermeasures are any human physiological (e.g., face, eyes, fingerprints-palm, or ECG) or behavioral (e.g., signature, voice, gait, or keystroke) patterns. As the PIN codes impede convenience and ease of access, the biometrics-based countermeasures are more popular today compared to the numbers-based countermeasures. Some recent smart mobile devices (e.g., iPhone 5S and up and Samsung Galaxy S5 and up) have started to integrate capacitive fingerprint scanners. As shown in Figure 4, we found 12 types of biometrics used as a countermeasure of attacks against authentication. Khamis et al. [84] used the *Gaze gestures* for shoulder-surfing resistant user authentication on smart mobile devices. Arteaga-Falconi et al. [57] and Kang et al. [58] used the *electrocardiogram* for biometrics authentication based on cross-correlation of the templates extracted. By recognizing the user's voice through the mic, Jeong et al. [52] used the *voice recognition* for user authentication in mobile cloud service architecture. From images captured by the front-facing cameras of smart mobile devices, Mahbub et al. [73] used the *face recognition* for continuous authentication. Based on the behavior of performing certain actions on the touch screens, Shahzad et al. [85] proposed the idea of using *Gestures and Signatures* to authenticate users on touch screen devices. Using gait captured from inertial sensors, Hoang et al. [61] proposed the *Gait recognition* with fuzzy commitment scheme for authentication systems. Based on the way and rhythm, in which the users interacts with a keyboard or keypad when typing characters, Kambourakis et al. [70] introduced the *Keystroke dynamics* for user authentication in smart mobile devices. In addition, Galdi et al. [43] introduced an authentication scheme using *iris recognition* and demonstrated its applicability on smart mobile devices. Finally, based on the idea that the instinctive gesture of responding to a phone call can be used to capture two different biometrics, Abate et al. [56] used the *ear* and *arm* gesture for user authentication in smart mobile devices.

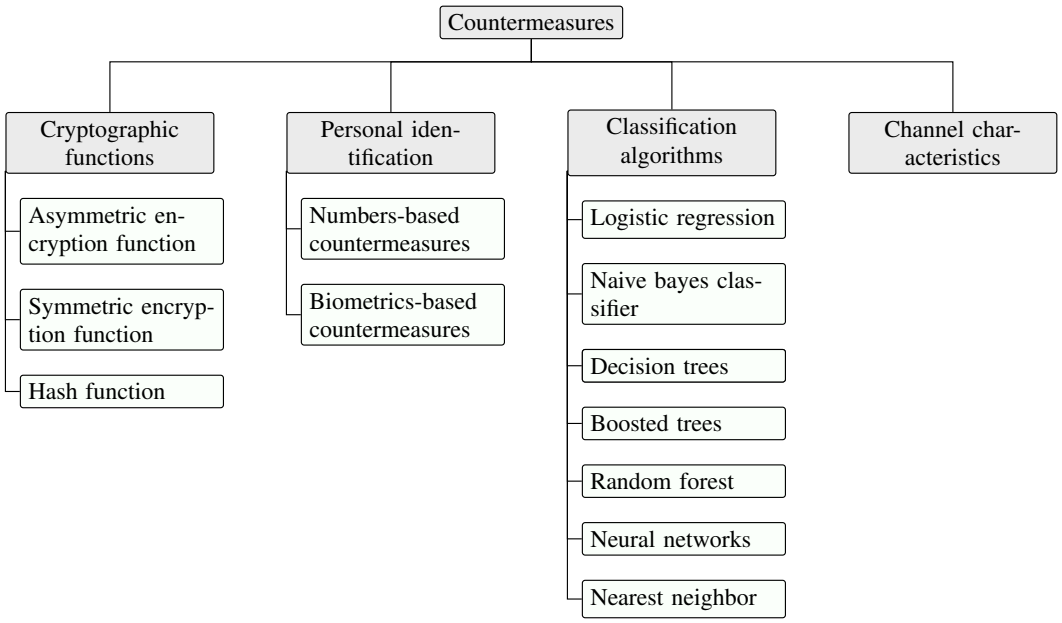

Fig. 3 Categorization of countermeasures used by the authentication schemes for smart mobile devices

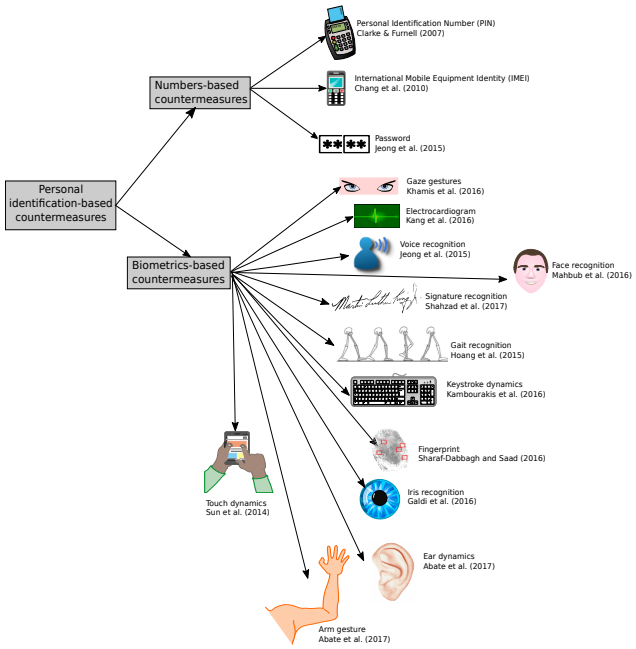

Fig. 4 Personal identification-based countermeasures used by the authentication schemes for smart mobile devices

4.2 Security analysis techniques

To prove the feasibility of authentication schemes for smart mobile devices in practice, researchers in the security field use security analysis techniques [87],[88], which can be categorized into five types, namely, computational assumptions, pattern recognition approaches, formal proof, random oracle model, and game theory, as shown in Figure 5. We note that the random oracle model can be classified into computational assumptions and formal proof. We circumvented this ambiguity by classifying the papers that use the random oracle model in a single category named "random oracle model".

The authentication schemes for smart mobile devices that use security analysis techniques are summarized in Table3. Note that the pattern recognition approaches are used especially by biometric-based authentication schemes. More precisely, Clarke and Furnell [54] used the pattern recognition approaches for evaluating the feasibility of utilizing keystroke information in classifying users. Kim and Hong [71] evaluated the feasibility of utilizing together teeth image and voice in terms of the training time per model and authentication time per image. Through the Sensor Pattern Noise (SPN), Galdi et al. showed that the sensor pattern noise-based technique can be reliably applied on smartphones. Wu and Tseng [36] used the random oracle model and computational assumptions to show that their proposed scheme is secure against ID attack. Finally, Liu et al. [47] used game theory concepts to prove that their proposed authentication scheme achieves anonymity, unlinkability, immunity of key-escrow, and mutual authentication.

In order to provide "provable security", Wang et al. [89] proposed the following five stages: 1) Definition of the threat model; 2) Definition of security goals; 3) selection of cryptographic assumptions; 4) Description of the main phases; and 5) Reductionist proof. Furthermore, there are two types of security analysis, namely, heuristic analysis and formal analysis. The role of heuristic analysis consists of discovery usability problems in any application, which can be found in the majority of antivirus solutions, while the role of formal analysis consists of analyzing and evaluating cryptographic

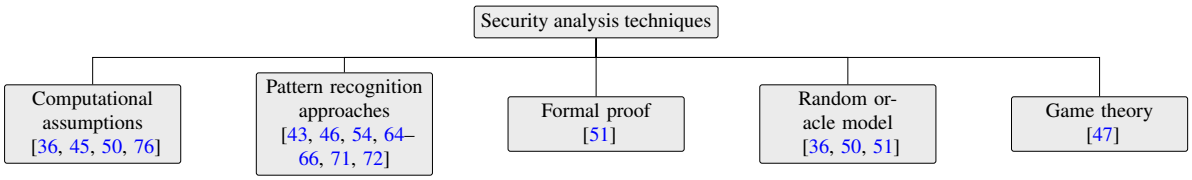

Fig. 5 Categorization of security analysis techniques used by the authentication schemes for smart mobile devices

Table 4 Notations used in comparison of computational costs

Notation	Definition
TAR	True acceptance rate
FAR	False acceptance rate
FRR	False rejection rate
ROC	Receiver operating characteristic
TPR	True-positive rate
FPR	False-positive rate
FNR	False-negative rate
EER	Equal error rate
GAR	Genuine acceptance rate
T_e	Ttime of executing a bilinear pairing operation
T_{mul}	Time of executing a multiplication operation of point
T_H	Time of executing a one-way hash function
T_{add}	Time of executing an addition operation of points
TE_{add}	Time of executing an elliptic curve point addition
TE_{mul}	Time of executing an elliptic curve point multiplication
TE_{inv}	Time of executing a modular inversion operation
C_1	Computational cost of client and server (total)
C_2	Computational cost of subscription (total)
T_{HE}	Time of encryption and decryption

protocols based on the security goals, which are defined in a formal model.

5 Authentication schemes for Smart Mobile Devices

Generally, the classification of authentication schemes frequently mentioned in the literature is done using the following three types, namely, Something-You-Know (can be shared and forgotten), Something-You-Have (can be shared and duplicated), and Someone-You-Are (not possible to share and repudiate), as discussed by Chen et al. in [13, 62]. In our work, according to the characteristics of the countermeasure that is used along with the authentication model, we categorize the authentication schemes for smart mobile devices in four categories, namely, 1) Biometric-based authentication schemes, 2) Channel-based authentication schemes, 3) Factor-based authentication schemes, and 4) ID-based authentication schemes, as shown in Figure 6. Inspired by the evaluation criteria presented in three recent works [93–95], we compare the authentication schemes of each category in term of security requirements. The table 6 presents a comparison of biometric-based authentication schemes for smart mobile devices in term of security requirements (CB1 to CB18). The table 8 presents a comparison of channel-based authentication schemes for smart mobile devices in term of security requirements (CC1 to CC10). The table 10 presents a comparison of factors-based authentication schemes for smart mobile devices in term of security requirements (CF1 to CF16). The table 11 presents a comparison of ID-based authentication schemes for smart mobile devices in term of security requirements (CI1 to CI18).

5.1 Biometric-based authentication schemes

The surveyed papers of biometric-based authentication schemes for smart mobile devices are shown in Table 5. As shown in Figure 7, the realization processes of a biometric-based authentication scheme for smart mobile devices are based on the following processes: 1) Definition of authentication model; 2) Definition of attacks model; 3) Selection of countermeasure; 4) Proposition of main phases of the scheme; 5) Security analysis techniques; and 6) Performance evaluation.

The behavioral biometric of Keystroke Dynamics analysis of the manner or rhythm in which an individual types characters on a keyboard or keypad is called keystroke analysis, and can be classified as either static or continuous. To authenticate users based on the keystroke analysis, Clarke and Furnell [53] introduced the concept of advanced user authentication, which is based on three interaction scenarios, namely, 1) Entry of 11-digit telephone numbers, 2) Entry of 4-digit PINs, and 3) Entry of text messages. The scheme in [53] can provide not only transparent authentication of the user and continuous or periodic authentication of the user, but it is also efficient in terms of false rejection rate and false acceptance rate under three type of mobile devices, namely, Sony Ericsson T68, HP IPAQ H5550, and Sony Clie PEG NZ90. To demonstrate the ability of neural network classifiers, the same authors in [54] proposed an authentication framework based on mobile handset keypads in order to support keystroke analysis. The three pattern recognition approaches used in this framework are, 1) Feed-forward multi-layered perceptron network, 2) Radial basis function network, and 3) Generalised regression neural network. Therefore, Maiorana et al. [67] proved that it is feasible to employ keystroke dynamics on mobile phones with the statistical classifier for keystroke recognition in order to employ it as a password hardening mechanism. In addition, the combination of time features and pressure features is proved by Tasia et al. in [69] that is the best one for authenticating users.

Fig. 6 Categorization of authentication schemes for smart mobile devices

Passwords that have been widely used by remote authentication schemes, can be easily guessed, hacked, and cracked. However, to overcome the drawbacks of only-password-based remote authentication, Khan et al. [33] proposed the concept of the chaotic hash-based fingerprint biometrics remote user authentication scheme. Theoretically, the scheme [33] can prevent from fives attacks, namely, parallel session attack, reflection attack, forgery attack, impersonation attack, DoS attack, and server spoofing attack, but it is not tested on mobile devices and it is vulnerable to biometric template attacks. To avoid the biometric template attack, Xi et al. [17] proposed an idea based on the transformation of the locally matched fuzzy vault index to the central server for biometric authentication using the public key infrastructure. Compared to [38], [33], and [17], Chen et al. [40] proposed an idea that uses only hashing functions on fingerprint

Table 5 Biometric-based authentication schemes for smart mobile devices

Time	Scheme	Method	Goal	Mobile device	Performance (+) and limitation (-)	Comp. complexity
2007	Clarke and Furnell [53]	- Keystroke analysis	- Introducing the concept of advanced user authentication	- Sony Ericsson T68; - HP IPAQ H5550; - Sony Clie PEG NZ90.	+ Keystroke latency - Process of continuous and non-intrusive authentication	Low
2007	Clarke and Furnell [54]	- Keystroke analysis	- Enable continuous and transparent identity verification	- Nokia 5110	+ GRNN has the largest spread of performances - The threat model is not defined	High
2008	Khan et al. [33]	- Fingerprint	- Introducing the concept of chaotic hash-based fingerprint biometrics remote user authentication scheme	- N/A	+ Can prevent from fives attacks, namely, parallel session attack, reflection attack, Forgery attack, impersonation attack, DoS attack, and server spoofing attack - The proposed scheme is not tested on mobile devices	Low
2010	Li and Hwang [37]	- Smart card	- Providing the non-repudiation	- N/A	+ Can prevent from three attacks, namely, masquerading attacks, replay attacks, and parallel session attacks - Storage costs are not considered	$10T_H$
2011	Xi et al. [17]	- Fingerprint	- Providing the authentication using bio-cryptographic	- Mobile device with Java Platform	+ Secure the genuine biometric feature - Server-side attack is not considered	at FAR=0.1% , GAR=78.69%
2012	Chen et al. [40]	- Fingerprint	- Using only hashing functions	- N/A	+ Solve asynchronous problem - Privacy-preserving is not considered	$7T_H$
2013	Frank et al. [72]	- Touchscreen	- Providing a behavioral biometric for continuous authentication	- Google Nexus One	+ Sufficient to authenticate a user - Not applicable for long-term authentication	11 to 12 strokes, EER=2%–3%
2014	Khan et al. [42]	- Fingerprint	- Improve the Chen et al.'s scheme and Truong et al.'s scheme	- N/A	+ Quick wrong password detection - Location privacy is not considered	$18T_H$
2015	Hoang et al. [61]	- Gait recognition	- Employing a fuzzy commitment scheme	- Google Nexus One	+ Efficient against brute force attacks - Privacy model is not defined	Low
2016	Arteaga-Falconi et al. [57]	- Electrocardiogram	- Introducing the concept of electrocardiogram-based authentication	- AliveCor	+ Concealing the biometric features during authentication - Privacy model is not considered.	TAR=81.82% and FAR=1.41%
2017	Abate et al. [56]	- Ear Shape	- Implicitly authenticate the person authentication	- Samsung Galaxy S4 smartphone	+ Implicit authentication - Process of continuous and non-intrusive authentication	EER=1%–1.13%
2018	Zhang et al. [96]	- Iris and periocular biometrics	- Develop a deep feature fusion network	- N/A	+ Requires much fewer storage spaces - The threat model is limited	EER= 0.60%

biometric remote authentication scheme to solve the asynchronous problem on mobile devices.

The biometric keys have some advantages, namely, 1) cannot be lost or forgotten, 2) very difficult to copy or share, 3) extremely hard to forge or distribute, and 4) cannot be guessed easily. In 2010, Li and Hwang [37] proposed a biometric-based remote user authentication scheme using smart cards, in order to provide the non-repudiation. Without storing password tables and identity tables in the system, Li and Hwang's scheme [37] can resist masquerading attacks, replay attacks, and parallel session attacks. Authors did not specify the application environment of their scheme, but it can be applied to smart mobile devices as the network model is not complicated. Note that Li and Hwang's scheme was cryptanalyzed several times. The question that we can ask is: is it possible to use a graphical password as an implicit password authentication system to avoid the screen-dump attacks? Almuairfi et al. [80] in 2013, introduced an image-based implicit password authentication system, named IPAS, which is based on creating a visualized image of a user's logged answers.

The touch dynamics for user authentication were initialed on desktop machines and finger identification machines. In 2012, Meng et al. [64] focused on a user behavioral biometric, namely touch dynamics such as touch duration and touch direction. Specifically, they proposed an authentication scheme that uses touch dynamics on touchscreen mobile phones. To classify users, Meng et al.'s scheme use known machine learning algorithms (e.g., Naive Bayes, decision tree) under an experiment with 20 users using Android touchscreen phones. Through simulations, the results show that Meng et al.'s scheme reduces the average error rate down to 2.92% (FAR of 2.5% and FRR of 3.34%). The question that we can ask is: is it possible to use the multi-touch as an authentication mechanism? Sae-Bae et al. [65] in 2012, introduced an authentication approach based on multi-touch gestures using an application on the iPad with version 3.2 of iOS. Compared with Meng et al.'s scheme [64], Sae-Bae et

Table 6 Comparison of biometric-based authentication schemes for smart mobile devices in term of security requirements (CB1 to CB18)

Scheme	CB1	CB2	CB3	CB4	CB5	CB6	CB7	CB8	CB9	CB10	CB11	CB12	CB13	CB14	CB15	CB16	CB17	CB18
Clarke and Furnell [53]	+	+	-	-	-	-	+	-	-	-	-	-	-	-	-	-	-	-
Clarke and Furnell [54]	+	+	-	-	-	-	+	-	-	-	-	-	-	-	-	-	-	-
Khan et al. [33]	-	+	+	+	+	+	+	+	-	+	-	-	-	-	-	-	-	-
Li and Hwang [37]	-	+	+	-	-	-	+	-	+	+	-	-	-	-	-	-	-	-
Xi et al. [17]	+	+	-	-	-	-	+	-	-	+	+	+	+	+	-	-	-	-
Chen et al. [40]	+	+	+	-	-	+	+	-	-	+	-	-	-	-	-	-	+	-
Frank et al. [72]	+	+	-	-	-	-	-	-	-	-	-	-	-	-	+	-	-	-
Khan et al. [42]	-	+	+	-	-	+	+	-	-	+	-	-	-	-	-	-	-	+
Hoang et al. [61]	+	+	-	-	-	-	-	-	-	-	-	+	-	-	-	-	-	-
Arteaga-Falconi et al. [57]	+	+	-	-	-	-	-	-	-	-	-	-	+	-	-	+	-	-
Abate et al. [56]	+	+	-	-	-	-	-	-	-	-	-	-	-	-	+	-	-	-
Zhang et al. [96]	-	+	-	-	-	-	-	-	-	-	-	-	-	-	+	-	-	-

(+) means the corresponding security requirement is achieved, while (-) not; CB1 : Evaluated on mobile devices ; CB2 : Provides the continuous and non-intrusive authentication; CB3: Resistance to parallel session attack; CB4: Resistance to reflection attack; CB5: Resistance to forgery attack; CB6: Resistance to impersonation attack; CB7: Resistance to DoS attack; CB8: Resistance to server spoofing attack; CB9: Resistance to masquerading attacks; CB10: Resistance to replay attacks; CB11: Secure the genuine biometric feature. CB12: Resistance to brute force attacks; CB13: The evaluation metric FAR is considered; CB14: The evaluation metric GAR is considered; CB15: The evaluation metric EER is considered; CB16: The evaluation metric TAR is considered; CB17: Solve asynchronous problem; CB18: Resistance to mobile device loss attack.

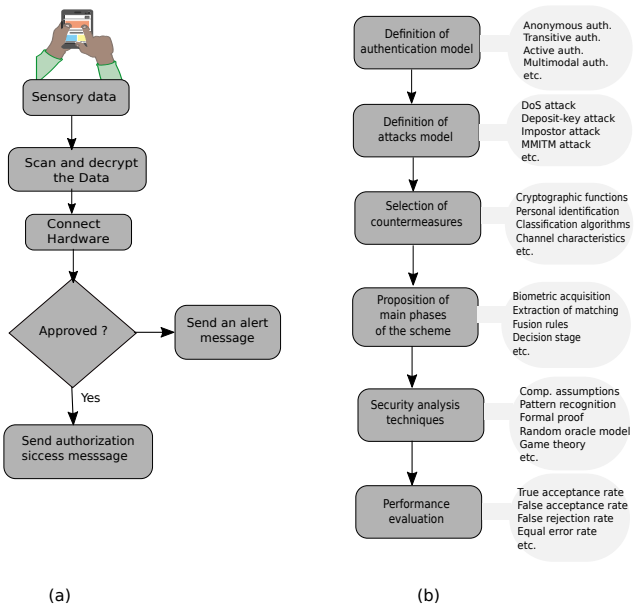

Fig. 7 Flowcharts depicting the process for (a) authentication using the biometrics-based countermeasures and (b) realization processes of an authentication scheme for smart mobile devices

al.'s approach is efficient with 10% EER on average for single gestures, and 5% EER on average for double gestures. Similar to Sae-Bae et al.'s approach [65], Feng et al. [66] designed a multi-touch gesture-based continuous authentication scheme, named FAST, that incurs FAR=4.66% and FRR= 0.13% for the continuous post-login user authentication. In addition, the FAST scheme can provide a good post-login access security, without disturbing the honest mobile users, but the threat model is very limited and privacy-preserving is not considered.

In 2016, Arteaga-Falconi et al. [57] introduced the concept of electrocardiogram-based authentication for mobile devices. Specifically, the authors considered five factors, namely, the number of electrodes, the quality of mobile ECG sensors, the time required to gain access to the phone, FAR, and TAR. Before applying the ECG authentication algorithm, the preprocessing stages for the ECG signal pass by the fiducial point detection. The ECG authentication algorithms are based on two aspects: 1) the use of feature-specific percentage of tolerance and 2) the adoption of a hierarchical validation scheme. The results reveal that the algorithm [57] has 1.41% false acceptance rate and 81.82% true acceptance rate with 4s of signal acquisition. Note that the ECG signals from mobile devices can be corrupted by noise as a result of movement and signal acquisition type, as discussed by Kang et al. [58]. However, the advantage of using ECG authentication is concealing the biometric features during authentication, but it is a serious problem if the privacy-preserving is not considered. Regarding the practical aspects of the smartphone approach in the ECG-authentication scheme, an individual heat pattern would be more practical if the smartphone could incorporate a heat camera.

Table 7 Channel-based authentication schemes for smart mobile devices

Time	Scheme	Method	Goal	Mobile device	Performance (+) and limitation (-)	Comp. complexity
2007	Varshavsky et al. [32]	- Physical proximity	- Authenticate co-located devices	- N/A	+ Not vulnerable to eavesdropping - The threat model is limited	High
2008	Li et al. [34]	- Electronic voting	- Introducing the concept of a deniable electronic voting authentication in MANETs	- N/A	+ Privacy requirement - Many assumptions needed to understand implementation	Medium
2011	He et al. [31]	- Seamless roaming	- Authenticate with privacy-preserving	- N/A	+ Privacy requirement - The threat model is limited	Medium
2013	Chen et al. [51]	- Tripartite authentication	- Establish a conference key securely	- Samsung Galaxy Nexus	+ Transitive authentication - Intrusion detection is not considered	Medium
2014	Guo et al. [48]	- Attribute-based authentication	- Authenticate with privacy-preserving	- Nexus S	+ Anonymity and untraceability - Interest privacy is not considered	High
2015	Seto et al. [63]	- User-habit-oriented authentication	- Integrate the habits with user authentication	- Google Nexus 4	+ More usable for people who have better memory for rhythms than for geometric curves - Privacy is not considered	High
2016	Yang et al. [46]	- Handover authentication	- Provides user anonymity and untraceability	- N/A	+ Access grant and data integrity - Many assumptions needed to understand implementation	Medium
2017	Samangouei et al. [97]	- Attribute-based authentication	- Introducing the concept of facial attributes for active authentication	- Google Nexus 5	+ Implemented with low memory usage - Intrusion detection and encryption are not considered	Medium
2018	Wu et al. [98]	- Private key security	- Provide both secure key agreement and private key security	- Samsung Galaxy S5	+ Perfect forward secrecy - Intrusion detection is not considered	Low

Table 8 Comparison of channel-based authentication schemes for smart mobile devices in term of security requirements (CC1 to CC10)

Scheme	CC1	CC2	CC3	CC4	CC5	CC6	CC7	CC8	CC9	CC10
Varshavsky et al. [32]	-	-	+	-	-	-	-	+	+	-
Li et al. [34]	-	+	+	-	-	-	-	+	+	+
He et al. [31]	-	+	+	-	-	-	-	+	+	-
Chen et al. [51]	+	+	+	-	-	-	-	+	+	-
Guo et al. [48]	+	+	+	-	-	-	+	+	+	-
Seto et al. [63]	+		+	-	-	-	-	+	+	-
Yang et al. [46]		+	+	+	+	+	+	+	+	-
Samangouei et al. [97]	+	-	+	-	-	-	-	-	-	-
Wu et al. [98]	+	+	+	+	+	+	+	+	+	-

(+) means the corresponding security requirement is achieved, while (-) not; CC1: Evaluated on mobile devices; CC2: Provides privacy-preserving; CC3: Provides transitive authentication; CC4: Provides anonymity; CC5: Provides untraceability; CC6: Provides access grant; Provides data integrity; CC7: Provides perfect forward secrecy; CC8: Resistance to passive attacks; CC9: Resistance to active attacks; CC10: Provides verifiability

5.2 Channel-based authentication schemes

The surveyed papers of channel-based authentication schemes for smart mobile devices are shown in Table 7. Focusing on dynamic characteristics of radio environment, Varshavsky et al. [32] showed that is possible to securely pair devices using the proximity-based authentication. Specifically, the authors proposed a technique to authenticate co-located devices, named, Amigo. The Amigo scheme uses the knowledge of the shared radio environment of devices as proof of physical proximity, which is specific to a particular location and time. Using the Diffie-Hellman key exchange with verification of device co-location, the Amigo scheme does not require user involvement to verify the validity of the authentication and can detect and avoid eavesdropping attacks such as the impostor attack and the man-in-the-middle attack. By exploiting physical layer characteristics unique to a body area network, Shi et al. [81] proposed a lightweight body area network authentication scheme, named BANA. Based on distinct received signal strength variations, the BANA scheme adopts clustering analysis to differentiate the signals from an attacker and a legitimate node. The advantage of BANA scheme is that it can accurately identify multiple attackers with the minimal amount of overhead.

As discussed by the work in [34], supporting group decisions and especially the electronic voting (e-voting) has become an important topic in the field of mobile applications, where the smart mobile devices can be used to make group decisions electronically. To secure e-voting system, Li et al. [34] proposed that an electronic voting protocol with deniable authentication should satisfy the following requirements: completeness, uniqueness, privacy, eligibility,

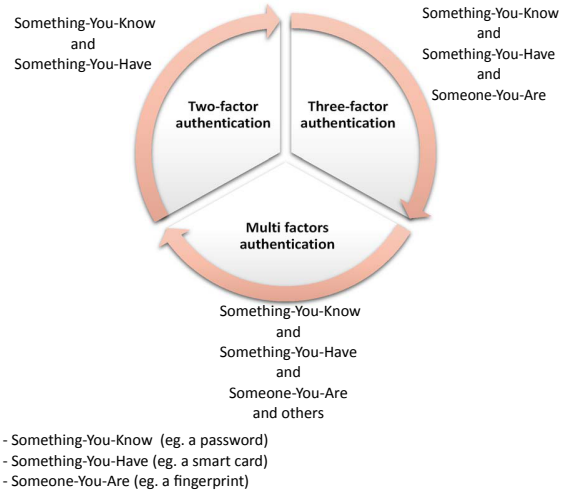

Fig. 8 Factors-based authentication schemes for smart mobile devices

fairness, verifiability, mobility, and deniable authentication. Based on three types of cryptography, namely, 1) asymmetric encryption function, 2) symmetric encryption function, and 3) hash function, the scheme [34] can meet these requirements of a secure e-voting system for application over mobile ad hoc networks. Theoretically, the scheme [34] can prevent four passive and active attacks, namely, man-in-the-middle attack, impersonation attack, replay attack, and eavesdropping attack, but many assumptions needed to understand the implementation in a smart mobile device.

A roaming scenario in wireless networks involves four parties, namely, a roaming user, a visiting foreign server, a home server, and a subscriber. He et al. [31] introduced a user authentication scheme with privacy-preserving, named Priauth, for seamless roaming over wireless networks. Based on probabilistic polynomial time algorithms, the Priauth scheme can satisfy the six requirements: (1) server authentication, (2) subscription validation, (3) provision of user revocation mechanism, (4) key establishment, (5) user anonymity, and (6) user untraceability, but the complexity is high when the Priauth scheme authenticates multiple handheld devices in ad-hoc environment. Using a temporary confidential channel, Chen et al. [51] proposed a bipartite and a tripartite authentication protocol to allow multiple handheld devices to establish a conference key securely, which can reduce the bottleneck of running time human's involvements.

To provide continuous secure services for mobile clients, it is necessary to design an efficient handover protocol that achieves the handover authentication with user anonymity and untraceability, as discussed in the work [46]. Specifically, Yang et al. use the identity-based elliptic curve algorithm for supporting user anonymity and untraceability in mobile cloud computing. To provide the active authentication on mobile devices, Samangouei et al. [97] introduced the concept of facial attributes.

5.3 Factor-based authentication schemes

The surveyed papers of factor-based authentication schemes for smart mobile devices are shown in Table 9. As shown in Figure 8, factor-based authentication can be classified into three types of categories, including, two-factor authentication, three-factor authentication, and multi-factor authentication.

Kim and Hong [71] proposed a multimodal biometric authentication approach using teeth image and voice. Specifically, this approach is based on two phases, namely, 1) teeth authentication phase and 2) voice authentication phase. The teeth authentication phase uses the AdaBoost algorithm based on Haar-like features for teeth region detection, and the embedded hidden Markov model with the two-dimensional discrete cosine transform. The voice authentication phase uses mel-frequency cepstral coefficients and pitch as voice features. Through performance evolution, the approach was shown that it is better than the performance obtained using teeth or voice individually, but the threat model is not defined. The question we ask here: is it sufficient to use an authentication approach without defining the threat models? Park et al. [38] showed that various attack routes in smart mobile devices may cause serious problems of privacy infringement in data protection. Specifically, using cryptographic methods, the authors designed a combined authentication and multilevel access control, named CAMAC. The CAMAC control uses three types of classification of information level, namely, 1) *Public*, which is not sensitive and can be disclosed in public, 2) *Not public but sharable*, which the data should be encrypted and be decrypted only by authorized users, and 3) *Not public and not sharable*, which the data should be decrypted only by the user himself/herself.

As discussed in the survey [18], MANET is an autonomous system of mobile nodes (e.g., smart mobile devices), which has several salient characteristics, namely, dynamic topologies, bandwidth constrained and energy constrained operation, and limited physical security. To authenticate the smart mobile devices in MANETs, Yu et al. [75] introduced the concept of multimodal biometric-based authentication, which uses a dynamic programming-based HMM scheduling algorithm to derive the optimal scheme. Therefore, the biosensor scheduling procedure used in the scheme [75] is based on three steps, namely, 1) Scheduling step, to find the optimal biosensor, 2) Observation step, to observe the output of the optimal biosensor and 3) Update step, to judge the result of the authentication. The scheme [75] is efficient in terms of biosensor costs, but the article fails to provide a detailed analysis of intrusion detection and encryption. Related to the scheme [75], Saevanee et al. [60] proposed a continuous user authentication using multi-modal biometrics with linguistic analysis, keystroke dynamics and behavioral profiling.

Table 9 Factors-based authentication schemes for smart mobile devices

Time	Scheme	Method	Goal	Mobile device	Performance (+) and limitation (-)	Comp. complexity
2008	Kim and Hong [71]	- Multimodal biometrics	- Authenticate using teeth image and voice	- Hp iPAQ rw6100	+ Better than the performance obtained using teeth or voice individually - The threat model is not defined	High
2008	Yu et al. [75]	- Multimodal biometrics	- Introducing the concept of multimodal biometric-based authentication in MANETs	- N/A	+ Biosensor costs - Intrusion detection and encryption are not considered	Medium
2010	Park et al. [38]	- Multilevel access control	- Control all accesses to the authorized level of database	- N/A	+ Flexibility to dynamic access authorization changes - Many assumptions needed to understand implementation	$10T_H$
2012	Chang et al. [68]	- Graphical password - KDA system	- Combine a graphical password with the KDA system	- Android devices	+ Suitable for low-power mobile devices - The threat model is limited	With thumbnails=3, FRR(%)=7.27, FAR(%)=5.73
2013	Crawford et al. [55]	- Keystroke dynamics - Speaker verification	- Integrate multiple behavioral biometrics with conventional authentication	- Android devices	+ Implement fine-grained access control - No suitable for low-power mobile devices	Medium
2014	Sun et al. [49]	- Multi-touch screens	- Authenticate using multi-touch mobile devices	- Google Nexus 7	+ Robust to shoulder-surfing and smudge attack - Anonymity problem	TPR=99.3% FPR=2.2%
2015	Chen et al. [62]	- Rhythm	- Authenticate using the rhythm for multi-touch mobile devices	- Google Nexus 7	+ More usable for people who have better memory for rhythms than for geometric curves - Privacy is not considered	FPR up to 0.7% FNR up to 4.2%
2016	Khamis et al. [84]	- Gaze gestures - Touch	- Allow passwords with multiple switches	- Android devices	+ Secure against side attacks - The threat model is not defined	Medium
2016	Sitova et al. [99]	- Hand movement, orientation, and grasp	- Authenticate using the grasp resistance and grasp stability	- Android devices	+ Continuous authentication - Cross-device interoperability	EER=15.1%
2017	Fridman et al. [100]	- Four biometric modalities	- Introducing the active authentication via four biometric modalities	- Android devices	+ Active authentication - User reparability	ERR=5% FRR =1,1%

Table 10 Comparison of factors-based authentication schemes for smart mobile devices in term of security requirements (CF1 to CF16)

Scheme	CF1	CF2	CF3	CF4	CF5	CF6	CF7	CF8	CF9	CF10	CF11	CF12	CF13	CF14	CF15	CF16
Kim and Hong [71]	+	+	+	-	-	-	-	-	-	-	-	-	-	-	-	-
Yu et al. [75]	-	+	+	-	-	-	-	-	-	-	-	-	-	-	-	-
Park et al. [38]	-	+	+	-	-	+	-	+	+	+	+	+	+	-	+	+
Chang et al. [68]	+	+	+	-	-	-	-	-	-	-	-	-	-	-	-	-
Crawford et al. [55]	+	+	+	-	-	-	-	-	-	-	-	-	-	-	-	-
Sun et al. [49]	+	+	+	+	+	-	-	-	-	-	-	-	-	-	-	-
Chen et al. [62]	+	+	+	+	+	-	-	-	-	-	-	-	-	-	-	-
Khamis et al. [84]	+	+	+	+	+	-	-	-	-	-	-	-	-	-	-	-
Sitova et al. [99]	+	+	+	+	+	-	-	-	-	-	-	-	-	+	-	-
Fridman et al. [100]	+	+	+	-	-	-	-	-	-	-	-	-	-	-	-	-

(+) means the corresponding security requirement is achieved, while (-) not; CF1: Evaluated on mobile devices; CF2: Provides multimodal biometric authentication; CF3: Provides continuous authentication; CF4: Resistance to shoulder-surfing attack; CF5: Resistance to smudge attack; CF6: Provides fine-grained access control; CF7: Secure against side attacks; CF8: Provides Privacy-preserving; CF9: Resistance to spoofing attack; CF10: Resistance to masquerading attack; CF11: Resistance to man-in-the-middle attack; CF12: Resistance to replay attack; CF13: Resistance to reflection attack; CF14: Resistance to population attacks; CF15: Provides confidentiality; CF16: Provides integrity.

Chang et al. [68] proposed the combination of a graphical password with the KDA (Keystroke Dynamic-based Authentication) system for touchscreen handheld mobile devices. The Chang et al.'s scheme uses the same three phases as in the KDA systems, namely, 1) Enrollment phase, 2) Classifier building phase, and 3) Authentication phase. The enrollment phase is launched when a user's finger presses the touchscreen of the handheld mobile device at thumbnail photo. The classifier building phase is used to verify the user's identity after obtaining the personal features, which the authors employ a computation-efficient statistical classifier proposed by Boechat et al. in [101]. In the authentication phase, the classifier is used to verify the user's identity where the system compares the sequence of graphical password with the registered one in the enrollment phase. Through the experiments, the probability of breaking the

Chang et al.'s scheme under a shoulder surfing attack is reduced.

Crawford et al. [55] proposed an extensible transparent authentication framework that integrates multiple behavioral biometrics, namely, keystroke dynamics and speaker verification. The processes of this framework are based on six phases, namely, 1) Update biometric input buffer, 2) Update explicit authentication buffer, 3) Compute individual biometric probability, 4) Compute device confidence, 5) Make task decision, and 6) Update training buffer and refresh classifiers. Therefore, the idea of capacitive touchscreen to scan body parts is proposed by Holz et al. in [61]. Specifically, the authors proposed a biometric authentication system, named Bodyprint, that detects users' biometric features using the same type of capacitive sensing. The Bodyprint system is implemented as an application on an LG Nexus 5 phone, which features a Synaptics ClearPad 3350 touch sensor.

Based on a multimodal recognition of face and iris, De Marsico et al. [82] designed an authentication application, named FIRME, to be embedded in mobile devices. The FIRME is made up of separate modules, with a common starting and final processing, and a central part specialized for each biometrics. The face recognition uses four phases, namely, 1) Acquisition and segmentation, 2) Spoofing detection, 3) Best template selection, and 4) Feature extraction and matching. The iris recognition uses two phases, namely, 1) Acquisition and segmentation and 2) Feature extraction and matching. The question we ask here is: Is it possible to use the iris liveness detection for mobile devices under the printed-iris attacks? The study published in 2015 by Gragnaniello et al. in [102] proves that with the local binary pattern descriptor, we can detect and avoid the printed-iris attacks using the classification through support vector machine with a linear kernel. Another question we ask here: Is FIRME's scheme effective for the partial face detection? The study published in 2016 by Mahbub et al. in [73] proves that with the fewer facial segment cascade classifiers, we can detect partially cropped and occluded faces captured using a smartphone's front-facing camera for continuous authentication.

The idea of a sequence of rhythmic taps/slides on a device screen to unlock the device is proposed by Chen et al. in [62]. Specifically, the authors proposed a rhythm-based two-factor authentication, named RhyAuth, for multi-touch mobile devices. The RhyAuth scheme is implemented as an application on Google Nexus 7 tablets powered by Android 4.2. Note that it is possible to use another factor as the third authentication factor such as ID/password. However, the question we ask here is: Is it possible to use four biometric modalities for mobile devices in order to authenticate the users? The study published in 2017 by Fridman et al. in [100] introduced the active authentication via four biometric modalities, namely, 1) text entered via soft keyboard, 2) applications used, 3) websites visited, and 4) physical location of the device as determined from GPS (when outdoors) or WiFi (when indoors).

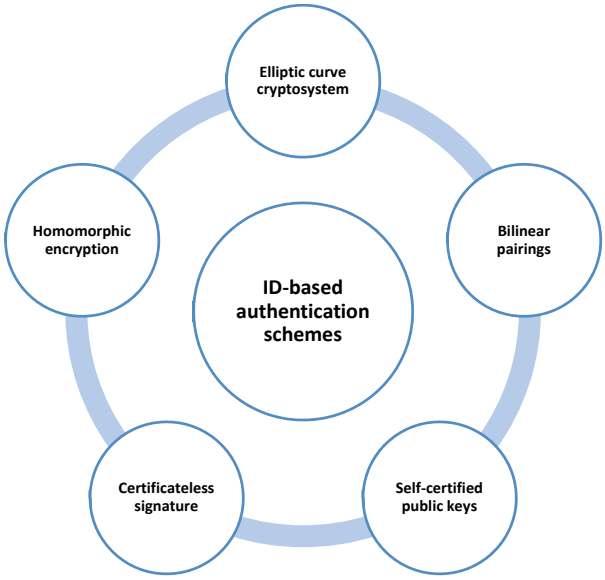

Fig. 9 Methods used to preserve the authentication models in ID-based authentication schemes for smart mobile devices

5.4 ID-based authentication schemes

The surveyed papers of ID-based schemes for smart mobile devices are shown in Table 12. With the application of cryptography in authentication schemes, smart mobile devices need additional computations, which causes the computation loads and the energy costs of mobile devices to be very high. To solve this problem, researchers proposed several ID-based authentication schemes using elliptic curve cryptosystem (ECC), as discussed in the work [16]. Therefore, as shown in Figure 9, there are five methods used to provide the authentication models in ID-based authentication schemes for smart mobile devices, namely, bilinear pairings, elliptic curve cryptosystem, self-certified public keys, certificateless signature, and homomorphic encryption.

Wang et al. [106] presented a good study of the challenges in designing a practical authentication scheme for mobile devices. Specifically, the study employs the following three identity-based remote user authentication schemes: Truong et al.'s scheme [107], Li et al.'s scheme [108], and Zhang et al.'s scheme [109]. The study provided the following three results: 1) Truong et al.'s scheme [107] is vulnerable to known session-specific temporary information attack, 2) Li et al.'s scheme [108] increases the management cost and communication overhead, and 3) Zhang et al.'s scheme [109] is susceptible to collusion attack and replay attack. In addition, the study highlight that "it is of great importance

Table 11 Comparison of ID-based authentication schemes for smart mobile devices in term of security requirements (CI1 to CI18)

Scheme	CI1	CI2	CI3	CI4	CI5	CI6	CI7	CI8	CI9	CI10	CI11	CI12	CI13	CI14	CI15	CI16	CI17	CI18
Yang and Chang [16]	-	+	+	+	+	+	-	+	+	+	-	-	-	+	-	-	-	-
Yoon and Yoo [35]	-	+	-	-	-	+	-	-	+	+	+	+	-	+	-	+	+	-
Wu and Tseng [36]	-	+	-	-	-	+	-	-	-	+	-	-	-	-	-	+	-	-
Sun and Leu [45]	+	+	-	-	-	-	+	-	+	-	-	-	+	+	-	-	-	-
Wu and Tseng [50]	-	+	-	-	-	+	-	-	-	+	-	-	-	+	-	+	+	-
Islam and Biswas [44]	-	+	-	-	-	+	-	-	-	+	-	+	-	+	-	+	-	-
He [76]	+	+	-	-	-	+	-	-	-	-	-	-	-	-	-	-	-	-
Liao and Hsiao [41]	+	+	-	-	-	+	-	-	+	+	-	-	-	+	-	+	+	-
Liu et al. [47]	+	+	-	-	-	-	-	-	+	+	-	-	-	+	-			+
Shahandashti et al. [83]	-	+	-	-	-	-	+	-	-	-	-	-	-	-	-	-	-	-
Islam and Khan [78]	-	+	-	-	-	+	+	-	-	-	-	-	-	-	-	-	-	-
Wu et al. [79]	-	+	-	-	-	+	+	-	+	+	-	-	-	+	-	+	-	-
Feng et al. [103]	+	+	-	-	-	+	+	-	+	+	-	+	-	+	-	-	-	-

(+) means the corresponding security requirement is achieved, while (-) not; CI1: Evaluated on mobile devices; CI2: Provides mutual authentication; CI3 : Provides reliability; CI4: The proposed scheme is flexible ; CI5: Provides high scalability ; CI6: Provides key agreement; CI7: Provides privacy-preserving ; CI8 : Resistance to outsider attack; CI9: Resistance to replay attack; CI10: Resistance to impersonation attack; CI11: Resistance to guessing attack; CI12: Resistance to stolen-verifier attack; CI13: Resistance to Forgery attack; CI14: Resistance to man-in-the-middle attack; CI15: Resistance to spoofing attack; CI16: Provides perfect forward secrecy; CI17: Provides session key security; CI18: Provides nonrepudiation.

to be aware of potential security threats when designing a protocol".

To provide the authentication of smart grid devices, Wang [110] proposed an identity-based data aggregation protocol, which they use an identity-based signature scheme with batch verification. The proposed protocol is robust against the following attacks: external attack, man-in-the-middle attack, internal attack, and replay attack. In addition, the proposed protocol provided security proof of batch verification. In some application scenarios, such as smart health, the identities of smart mobile devices may disclose the privacy of users. The work by Wang [111] proposed a privacy-preserving and accountable authentication protocol for IoT end-devices with weaker identity. The proposed protocol uses a secret sharing scheme as well as a group signature to provide the authentication for end-devices with weak identity.

In order to provide mutual authentication or a session key agreement, Yang and Chang [16] presented an ID-based remote mutual authentication with key agreement scheme. Specifically, the scheme is based on three phases, namely, system initialization phase, user registration phase, and mutual authentication with key agreement phase. Based on the analysis of computational and communication costs, the scheme [16] is efficient compared to Jia et al.'s scheme [92] and can resist outsider, impersonation, and replay attacks. Therefore, Islam and Biswas [44] have analyzed the disadvantage of Yang and Chang's scheme [16] and found that is inability to protect user's anonymity, known session-specific temporary information attack, and clock synchronization problem.

Yoon and Yoo's scheme [35] showed that Yang and Chang's scheme [16] is vulnerable to an impersonation attack and does not provide perfect forward secrecy. Similar to both Yang and Chang's scheme [16] and Yoon and Yoo's scheme [35], Wu and Tseng [36] proposed an ID-based mutual authentication and key exchange scheme for low-power mobile devices. Using the random oracle model and under the gap Diffie–Hellman group, Wu and Tseng's scheme is secure against an ID attack, impersonation attack, and passive attack. The question we ask here is: Will resistance to the impersonation attack provide the desired reliability of an authentication scheme for smart mobile devices? The new study published in 2017 by Spreitzer et al. in [25] proved that the transition between local attacks and vicinity attacks can be increased under the local side-channel attacks, especially in case of passive attacks. Thereby, the local side-channel attacks need to be studied by the authentication schemes for smart mobile devices.

To provide anonymous authentication in mobile pay-TV systems, Sun and Leu [45] proposed an authentication scheme in order to protect the identity privacy. Based on Elliptic curve cryptography (ECC), the Sun and Leu's scheme can manipulate authentication parameters and authorization keys for the multiple requests. Related to the scheme [45], HE et al. [77] proposed a one-to-many authentication scheme for access control in mobile pay-TV systems. Therefore, using four mechanisms, namely, symmetrical cryptosystem, asymmetrical cryptosystem, digital signature and one-way hash function, Chen's scheme [112] proposed an effective digital right management scheme for mobile devices. Note that Chang et al. [39] have found that Chen's scheme [112] is insecure because an attacker can easily compute the symmetric key, and they proposed an improved schema based on

Table 12 ID-based authentication schemes for smart mobile devices

Time	Scheme	Method	Goal	Mobile device	Performance (+) and limitation (-)	Comp. complexity
2009	Yang and Chang [16]	- Elliptic curve cryptosystem	- Providing mutual authentication with key agreement	- N/A	+ Resist to outsider, impersonation, and replay attacks - Perfect forward secrecy is not considered compared to the Yoon and Yoo's scheme [35]	$3TE_{mul} + 2TE_{add}$
2009	Yoon and Yoo [35]	- Elliptic curve cryptosystem	- Providing the perfect forward secrecy	- N/A	+ Session key security - Location privacy is not considered	$1TE_{mul} + 2TE_{add}$
2009	Wu and Tseng [36]	- Bilinear pairings	- Providing the implicit key confirmation and partial forward secrecy	- N/A	+ Secure against a passive attack - The proposed scheme is not tested on mobile devices	$C_1 = 2T_e + 5T_{mul} + 8T_H + T_{add}$
2009	Sun and Leu [45]	- Elliptic curve cryptography	- Providing one-to-many facility	- Mobile Pay-TV system	+ Resisting man-in-the-middle attack and replay attack - Interest privacy is not considered	$C_2 = 7T_e + 8T_{mul}$
2010	Wu and Tseng [50]	- Bilinear pairings	- Providing the implicit key confirmation and partial forward secrecy	- N/A	+ Secure against ID attack - The average message delay and the verification delay are not evaluated	$C_1 = 2T_e + 6T_{mul} + 6T_H + 2T_{add}$
2011	Islam and Biswas [44]	- Elliptic curve cryptosystem	- Improve the Yang and Chang's scheme [16]	- N/A	+ Prevents user's anonymity problem - Vulnerable to the ephemeral-secret-leakage attacks	$C_1 = 4T_{add} + 8T_{mul} + 7T_H$
2012	He [76]	- Bilinear pairings	- Providing the key agreement and mutual authentication	- HiPerSmart	+ Provides key agreement - Perfect forward secrecy is not considered compared to the Yoon and Yoo's scheme [35]	$C_1 = 2T_{add} + 5T_{mul} + 4T_H + T_e + TE_{inv}$
2013	Liao and Hsiao [41]	- Self-certified public keys	- Eliminate the risk of leaking the master secret key	- HiPerSmart	+ User reparability - Anonymity problem	$C_1 = 2T_{add} + 10T_{mul} + 7T_H + 2T_e$
2014	Liu et al. [47]	- Certificateless signature	- Avoiding the forgery on adaptively chosen message attack	- Windows CE 5.2 OS	+ Privacy of potential WBAN users - The threat model is limited	$C_1 = 3T_e + 2T_{mul} + 6T_H + 2T_{add}$
2015	Shahandashti et al. [83]	- Homomorphic encryption	- Achieving implicit authentication	- N/A	+ Secure against maliciously-controlled devices - Vulnerable to the replay attack	Medium
2016	Islam and Khan [78]	- Elliptic curve cryptosystem	- Providing the user anonymity and unlinkability	- N/A	+ Resistance to Pohlig–Hellman attack - Location privacy is not considered	$C_2 = 8TE_{mul}$
2017	Wu et al. [79]	- Elliptic curve cryptosystem	- Providing the user anonymity and privacy-preserving	- N/A	+ Perfect forward secrecy - Vulnerable to the ephemeral-secret-leakage attacks	$C_1 = 4TE_{mul} + 11T_H$
2018	Feng et al. [103]	- Lattice-based anonymous authentication	- Implement an anonymous authentication for the postquantum world	- Samsung GT-I9300	+ Satisfies the identity anonymity and unlinkability characteristics - Interest privacy is not considered	Low

three phases: the registration phase, the package phase, and the enhanced authorization phase.

6 Open Research Issues and Lessons learned

Table 13 summarizes the future directions in authentication issues for smart mobile devices.

6.1 Android malware or malfunctioning smart mobile devices

In 2016 [113, 114], an Android malware succeeded in bypassing the two-factor authentication scheme of many banking mobile apps. The malware can steal the user's login credential, including the SMS verification code. When the legitimate application is launched, the malware is triggered and a fake login screen overlays the original mobile banking one, with no option to close it. After that, the user fills in their personal data in the fake app. The key success of this attack is based on the phishing technique, which displays a graphical user interface (GUI) that has similar visual features as the legitimate app. The malware can also intercept two-factor authentication code (i.e., verification code sent through SMS), and forward it to the attacker. One research direction to prevent this kind of attacks is to detect the apps which have similar visual appearance and are installed on the same mobile device.

6.2 Rethinking authentication on smart mobile devices

Mobile devices are nowadays an essential part of our everyday life and can be integrated with different types of networks such as IoT, vehicular networks, smart grids, ...etc. as they help the user accessing the required resources and information of these networks. This integration requires rethinking the authentication protocols already proposed for mobile devices and considers the new architecture, the new

Table 13 Summary of Open Research Issues

Challenges	Description	Focus/Objective	Contribution	Research opportunities
False data injection attacks in mobile cyber-physical system	False data injection attacks jeopardize the system operations in smart mobile devices	How to identify and mitigate false data injection attacks in the mobile cyber-physical system?	Conventional false data detection approaches	- How to evaluate the overall running status? - How to design a reputation system with an adaptive reputation updating?
Analysis of smart mobile devices under topology attacks	Malicious attacker steals the topology	How to identify the topology attacks and reduce the amount of stolen information	A stochastic Petri net approach	- How to proof the efficacy of using a stochastic Petri net approach ? - How to prove that Petri nets can be useful for modeling mobile cyber-physical system?
Integration of smart mobile devices using new generation optical infrastructure technologies (NGN)	Integration of smart mobile devices with different types of networks such as IoT, vehicular networks, smart grids, ...etc.	How the smart mobile devices are able to mutually authenticate with NGN without any significant increase in overheads ?	An energy-aware encryption for smart mobile devices in Internet of Multimedia Things	- How to integrate smart mobile devices into NGN ? - How to design an authentication scheme that reduces the costs in terms of storage cost, computation complexity, communication overhead, and delay overhead?
Android malware or malfunctioning smart mobile devices	Malicious or malfunctioning smart mobile devices can be the source of data	How to safeguard data against such attacks?	An efficient end-to-end security and encrypted data scheme	- The choice of encryption is a challenge in view of power complexities of smart mobile devices
Anonymous profile matching	Malicious or malfunctioning smart mobile devices identify a user who has the same profiles	How to provides the conditional anonymity ?	Prediction-based adaptive pseudonym change strategy	- How to keeps the service overhead of mobile devices very low? - How to achieve the confidentiality of user profiles? - How to resist against the false data injection from the external attacks ?
Group authentication and key agreement security under the 5G network architecture	A group of smart mobile devices accessing the 5G network simultaneously cause severe authentication issues	Rethinking the authentication and key agreement protocols in 3G/LTE networks	A group authentication scheme based on Elliptic Curve Diffie-Hellman (ECDH) to realize key forward/backward secrecy	- How to provide privacy and key forward/backward secrecy? - How to resist the existing attacks including redirection, man-in-the-middle, and denial-of-service attacks, etc.
Electrocardiogram-based authentication with privacy preservation for smart mobile devices	Privacy preservation in electrocardiogram-based authentication remains a challenging problem since adversaries can find different ways of exploiting vulnerabilities of the electrocardiogram system	- How to reduce the acquisition time of Electrocardiogram signals for authentication ? - How to achieve privacy preservation and electrocardiogram integrity with differential privacy and fault tolerance?	- Proposing new privacy-preserving aggregation algorithms - Proposing a new secure handover session key management scheme	- How to resist sensing data link attack? - How to achieve scalability by performing aggregation operations ? - How to improve the TAR and FAR using deep learning?
Authentication for smart mobile devices using Software-defined networking (SDN) and network function virtualization (NFV)	The development of network functions using SDN/NFV remains a challenging problem since mobile malware can disrupt the operation of the protocols between the control and data planes, e.g., OpenFlow [104] and ForCES [105]	- How to achieve mutual authentication by adopting both SDN and NFV technologies?	- Proposing new private data aggregation scheme for authentication	- How to secure against malware attack? - How to achieve the computation efficiency?

threats, as well as the implementation feasibility in case of resource-constrained devices.

6.3 Developing more robust containers against sophisticated attacks

Employees work very often with their mobile devices by using electronic mail, exchange IM messages (instant messaging) or view files directly on the cloud through an online cloud storage application. This means that corporate data are at high risk unless we take the necessary measures to ensure that data are protected and safe. One solution is to secure files with the use of a secure container. Containers isolate user's mobile device and emails are encrypted for protection against third-party access and attachments to emails open in the container, in order to prevent leakage to third-party applications. Future research should focus on developing more robust containers against sophisticated attacks or implementing secure App Wrapping techniques.

6.4 Securing mobile devices based on unsolvable puzzle

Recently, University of Michigan was funded for producing a computer that is unhackable [115]. MORPHEUS outlines a new way to design hardware so that information is rapidly and randomly moved and destroyed. The technology works to elude attackers from the critical information they need to construct a successful attack. It could protect both hardware and software. This idea can be the basis for future research for securing mobile devices from attackers.

6.5 Combined intrusion detection and authentication scheme in smart mobile devices

Intrusion detection capabilities can be built inside the mobile devices in order to spot real-time malicious behaviors. Such techniques must use combined characteristics and exploit and social network analysis techniques [116], in order to cope with zero day attacks and small fluctuations in user behavior. There are many types of algorithms that may be used to mine audit data on real time, that can be applied to mobile devices. Data mining based IDSs have demonstrated higher accuracy, to novel types of intrusion and robust behaviour [117].

6.6 False data injection attacks in mobile cyber-physical system

False data injection attacks are crucial security threats to the mobile cyber-physical system, where the attacker can jeopardize the system operations in smart mobile devices. Recently, Li et al. in [118] proposed a distributed host-based collaborative detection scheme to detect smart false data injection attacks white low false alarm rate. To identify anomalous measurement data reported, the proposed scheme employs a set of rule specifications. However, how to identify and mitigate false data injection attacks in the mobile cyber-physical system? Hence, countermeasures for false data injection attacks in the mobile cyber-physical system should be researched in the future.

6.7 Group authentication and key agreement security under the 5G network architecture

Based on recent advances in wireless and networking technologies such as Software-defined networking (SDN) and network function virtualization (NFV), 5G will enable a fully mobile and connected society. According to Nguyen et al. [119], the development of network functions using SDN and NFV will achieve an extremely high data rate. On the other hand, a group of smart mobile devices accessing the 5G network simultaneously causes severe authentication issues. In a work published in 2018, Ferrag et al. [87] categorized threat models in cellular networks in four categories, namely, attacks against privacy, attacks against integrity, attacks against availability, and attacks against authentication. How to achieve mutual authentication by adopting both SDN and NFV technologies under these threat models? One possible future direction is to develop a group authentication scheme based on Elliptic Curve Diffie-Hellman (ECDH) to realize key forward/backward secrecy.

6.8 Electrocardiogram-based authentication with privacy preservation for smart mobile devices

Privacy preservation in electrocardiogram-based authentication remains a challenging problem since adversaries can find different ways of exploiting vulnerabilities of the electrocardiogram system. Two questions we ask here: How to reduce the acquisition time of Electrocardiogram signals for authentication? and how to achieve privacy preservation and electrocardiogram integrity with differential privacy and fault tolerance? A possible research direction in this topic could be related to proposing new privacy-preserving aggregation algorithms to resist sensing data link attack.

6.9 Lessons learned

Based on the aforementioned research and analysis that we conducted, we propose the following eight-step process for proposing an efficient authentication scheme for smart mobile devices. This process can be run in multiple cycles depending on the validation and evaluation outcomes or the new characteristics of the system (e.g. new nodes entering the system, new network connections, etc..

1. Definition of the network environment that smart mobile devices are used (e.g., Internet of Vehicles, Internet of Sensors, Internet of Energy,... etc.).
2. Definition of authentication models that can be used (anonymous authentication, transitive authentication, active authentication, multimodal authentication,... etc.).
3. Definition of attacks models (e.g., identity-based attacks, eavesdropping-based attacks, Combined eavesdropping and identity-based attacks, manipulation-based attacks, and service-based attacks).
4. Identification of areas of vulnerability and possible interdependencies of the system.
5. Selection of countermeasures (cryptographic functions, personal identification, classification algorithms, channel characteristics,...etc.).
6. Proposition of the main phases of the scheme (biometric acquisition, extraction of matching, fusion rules, decision stage,... etc.).
7. Security analysis techniques used for validating the efficiency of the proposed method(computational assumptions, pattern recognition approaches, formal proof, random oracle model, game theory,...etc.).
8. Performance evaluation (User side computational cost, server side computational cost, true acceptance rate, false acceptance rate, false rejection rate, equal error rate,...etc.).

This eight step process can be integrated in the cybersecurity life-cycle that every organization must follow in order to secure its systems (Prediction, Protection, Detection, Re-

action [120]) and can be either combined with agile software development principles [121].

7 Conclusions

In this article, we surveyed the state-of-the-art of authentication schemes for smart mobile devices. Through an extensive research and analysis that was conducted, we were able to classify the threat models in smart mobile devices into five categories, including, identity-based attacks, eavesdropping-based attacks, combined eavesdropping and identity-based attacks, manipulation-based attacks, and service-based attacks. In addition, we were able to classify the countermeasures into four types of categories, including, cryptographic functions, personal identification, classification algorithms, and channel characteristics. Regarding the cryptographic functions, the surveyed schemes use three types of cryptographic functions, including, asymmetric encryption function, symmetric encryption function, and hash function.

In order to ensure authentication by the personal identification, the surveyed schemes use two types, including, 1) biometrics-based countermeasures, which are any human physiological (e.g., face, eyes, fingerprints-palm, or ECG) or behavioral (e.g., signature, voice, gait, or keystroke pattern); 2) numbers-based countermeasures (e.g, Personal Identification Number (PIN), International Mobile Equipment Identity (IMEI), and Password). From security analysis perspective, there are five security analysis techniques used in authentication for smart mobile devices, namely, computational assumptions, pattern recognition approaches, formal proof, random oracle model, and game theory.

According to the countermeasure characteristic and the authentication model used, we were able to classify the surveyed schemes for smart mobile devices in four categories, namely, biometric-based authentication schemes, channel-based authentication schemes, factor-based authentication schemes, and ID-based authentication schemes. In addition, we presented a side-by-side comparison in a tabular form for each category, in terms of performance, limitations, and computational complexity.

There are still several challenging research areas (e.g., false data injection attacks in mobile cyber-physical system, analysis of smart mobile devices under topology attacks, Group authentication and key agreement security under the 5G network architecture, and electrocardiogram-based authentication with privacy preservation...etc), which can be further investigated in the near future.

References

1. Thuemmler C, Bai C (eds) (2017) Health 4.0: How Virtualization and Big Data are Revolutionizing Healthcare. Springer International Publishing, Cham, DOI 10.1007/978-3-319-47617-9
2. Ferrag MA, Maglaras LA, Janicke H, Jiang J, Shu L (2017) Authentication Protocols for Internet of Things: A Comprehensive Survey. Secur Commun Networks 2017:1–41, DOI 10.1155/2017/6562953
3. Khan WZ, Xiang Y, Aalsalem MY, Arshad Q (2013) Mobile Phone Sensing Systems: A Survey. IEEE Commun Surv Tutorials 15(1):402–427, DOI 10.1109/SURV.2012.031412.00077
4. Ferrag MA (2017) Epec: an efficient privacy-preserving energy consumption scheme for smart grid communications. Telecommunication Systems 66(4):671–688
5. Ferrag MA, Nafa M, Ghanemi S (2013) Ecpdr: An efficient conditional privacy-preservation scheme with demand response for secure ad hoc social communications. International Journal of Embedded and Real-Time Communication Systems (IJERTCS) 4(3):43–71
6. Qin Z, Sun J, Wahaballa A, Zheng W, Xiong H, Qin Z (2017) A secure and privacy-preserving mobile wallet with outsourced verification in cloud computing. Comput Stand Interfaces 54:55–60, DOI 10.1016/j.csi.2016.11.012
7. Pappel I, Pappel I, Tepandi J, Draheim D (2017) Systematic Digital Signing in Estonian e-Government Processes. In: Trans. Large-Scale Data-and Knowledge-Centered Syst. XXXVI, Springer, pp 31–51
8. Schünemann WJ, Baumann MO (eds) (2017) Privacy, Data Protection and Cybersecurity in Europe. Springer International Publishing, Cham, DOI 10.1007/978-3-319-53634-7
9. Ferrag MA, Maglaras L, Derhab A (2019) Authentication and authorization for mobile iot devices using biofeatures: Recent advances and future trends. Security and Communication Networks 2019
10. Ferrag MA, Maglaras L, Derhab A, Korba AA (2018) Taxonomy of biometric-based authentication schemes for mobile computing devices. In: 2018 3rd International Conference on Pattern Analysis and Intelligent Systems (PAIS), IEEE, pp 1–8
11. Patel VM, Chellappa R, Chandra D, Barbello B (2016) Continuous User Authentication on Mobile Devices: Recent progress and remaining challenges. IEEE Signal Process Mag 33(4):49–61, DOI 10.1109/MSP.2016.2555335
12. Evans M, Maglaras LA, He Y, Janicke H (2016) Human behaviour as an aspect of cybersecurity assurance. Secur Commun Networks 9(17):4667–4679, DOI 10.1002/sec.1657
13. Meng W, Wong DS, Furnell S, Zhou J (2015) Surveying the Development of Biometric User Authen-

tication on Mobile Phones. IEEE Commun Surv Tutorials 17(3):1268–1293, DOI 10.1109/COMST.2014.2386915
14. Meng Y, Wong DS, Schlegel R, Kwok Lf (2013) Touch Gestures Based Biometric Authentication Scheme for Touchscreen Mobile Phones. pp 331–350, DOI 10.1007/978-3-642-38519-3_21
15. Li S, Ashok A, Zhang Y, Xu C, Lindqvist J, Gruteser M (2016) Whose move is it anyway? Authenticating smart wearable devices using unique head movement patterns. In: 2016 IEEE Int. Conf. Pervasive Comput. Commun., IEEE, pp 1–9, DOI 10.1109/PERCOM.2016.7456514
16. Yang JH, Chang CC (2009) An ID-based remote mutual authentication with key agreement scheme for mobile devices on elliptic curve cryptosystem. Comput Secur 28(3-4):138–143, DOI 10.1016/j.cose.2008.11.008
17. Xi K, Ahmad T, Han F, Hu J (2011) A fingerprint based bio-cryptographic security protocol designed for client/server authentication in mobile computing environment. Secur Commun Networks 4(5):487–499, DOI 10.1002/sec.225
18. Ferrag MA, Maglaras L, Ahmim A (2017) Privacy-Preserving Schemes for Ad Hoc Social Networks: A Survey. IEEE Commun Surv Tutorials 19(4):3015–3045, DOI 10.1109/COMST.2017.2718178
19. La Polla M, Martinelli F, Sgandurra D (2013) A Survey on Security for Mobile Devices. IEEE Commun Surv Tutorials 15(1):446–471, DOI 10.1109/SURV.2012.013012.00028
20. A Harris M, P Patten K (2014) Mobile device security considerations for small- and medium-sized enterprise business mobility. Inf Manag Comput Secur 22(1):97–114, DOI 10.1108/IMCS-03-2013-0019
21. Faruki P, Bharmal A, Laxmi V, Ganmoor V, Gaur MS, Conti M, Rajarajan M (2015) Android Security: A Survey of Issues, Malware Penetration, and Defenses. IEEE Commun Surv Tutorials 17(2):998–1022, DOI 10.1109/COMST.2014.2386139
22. Teh PS, Zhang N, Teoh ABJ, Chen K (2016) A survey on touch dynamics authentication in mobile devices. Comput Secur 59:210–235, DOI 10.1016/j.cose.2016.03.003
23. Alizadeh M, Abolfazli S, Zamani M, Baharun S, Sakurai K (2016) Authentication in mobile cloud computing: A survey. J Netw Comput Appl 61:59–80, DOI 10.1016/j.jnca.2015.10.005
24. Gandotra P, Kumar Jha R, Jain S (2017) A survey on device-to-device (D2D) communication: Architecture and security issues. J Netw Comput Appl 78:9–29, DOI 10.1016/j.jnca.2016.11.002
25. Spreitzer R, Moonsamy V, Korak T, Mangard S (2017) Systematic Classification of Side-Channel Attacks: A Case Study for Mobile Devices. IEEE Commun Surv Tutorials pp 1–1, DOI 10.1109/COMST.2017.2779824
26. Kunda D, Chishimba M (2018) A survey of android mobile phone authentication schemes. Mobile Networks and Applications pp 1–9
27. Aslam MU, Derhab A, Saleem K, Abbas H, Orgun M, Iqbal W, Aslam B (2017) A Survey of Authentication Schemes in Telecare Medicine Information Systems. J Med Syst 41(1):14, DOI 10.1007/s10916-016-0658-3
28. Velásquez I, Caro A, Rodríguez A (2018) Authentication schemes and methods: A systematic literature review. Inf Softw Technol 94:30–37, DOI 10.1016/j.infsof.2017.09.012
29. Kilinc HH, Yanik T (2014) A Survey of SIP Authentication and Key Agreement Schemes. IEEE Commun Surv Tutorials 16(2):1005–1023, DOI 10.1109/SURV.2013.091513.00050
30. Wang D, Shen J, Liu JK, Choo KKR (2018) Rethinking authentication on smart mobile devices. Wireless Communications and Mobile Computing 2018, DOI 10.1155/2018/7079037
31. He D, Bu J, Chan S, Chen C, Yin M (2011) Privacy-Preserving Universal Authentication Protocol for Wireless Communications. IEEE Trans Wirel Commun 10(2):431–436, DOI 10.1109/TWC.2010.120610.101018
32. Varshavsky A, Scannell A, LaMarca A, de Lara E (2007) Amigo: Proximity-Based Authentication of Mobile Devices. In: UbiComp 2007 Ubiquitous Comput., pp 253–270, DOI 10.1007/978-3-540-74853-3_15
33. Khan MK, Zhang J, Wang X (2008) Chaotic hash-based fingerprint biometric remote user authentication scheme on mobile devices. Chaos, Solitons & Fractals 35(3):519–524, DOI 10.1016/j.chaos.2006.05.061
34. Li CT, Hwang MS, Liu CY (2008) An electronic voting protocol with deniable authentication for mobile ad hoc networks. Comput Commun 31(10):2534–2540, DOI 10.1016/j.comcom.2008.03.018
35. Yoon EJ, Yoo KY (2009) Robust ID-Based Remote Mutual Authentication with Key Agreement Scheme for Mobile Devices on ECC. In: 2009 Int. Conf. Comput. Sci. Eng., IEEE, pp 633–640, DOI 10.1109/CSE.2009.363
36. Wu TY, Tseng YM (2010) An ID-Based Mutual Authentication and Key Exchange Protocol for Low-Power Mobile Devices. Comput J 53(7):1062–1070, DOI 10.1093/comjnl/bxp083
37. Li CT, Hwang MS (2010) An efficient biometrics-based remote user authentication scheme using smart

cards. J Netw Comput Appl 33(1):1–5, DOI 10.1016/j.jnca.2009.08.001
38. Hyun-A Park, Jong Wook Hong, Jae Hyun Park, Zhan J, Dong Hoon Lee (2010) Combined Authentication-Based Multilevel Access Control in Mobile Application for DailyLifeService. IEEE Trans Mob Comput 9(6):824–837, DOI 10.1109/TMC.2010.30
39. Chang CC, Yang JH, Wang DW (2010) An efficient and reliable E-DRM scheme for mobile environments. Expert Syst Appl 37(9):6176–6181, DOI 10.1016/j.eswa.2010.02.110
40. Chen CL, Lee CC, Hsu CY (2012) Mobile device integration of a fingerprint biometric remote authentication scheme. Int J Commun Syst 25(5):585–597, DOI 10.1002/dac.1277
41. Liao YP, Hsiao CM (2013) A novel multi-server remote user authentication scheme using self-certified public keys for mobile clients. Futur Gener Comput Syst 29(3):886–900, DOI 10.1016/j.future.2012.03.017
42. Khan MK, Kumari S, Gupta MK (2014) More efficient key-hash based fingerprint remote authentication scheme using mobile device. Computing 96(9):793–816, DOI 10.1007/s00607-013-0308-2
43. Galdi C, Nappi M, Dugelay JL (2016) Multimodal authentication on smartphones: Combining iris and sensor recognition for a double check of user identity. Pattern Recognit Lett 82:144–153, DOI 10.1016/j.patrec.2015.09.009
44. Islam SH, Biswas G (2011) A more efficient and secure ID-based remote mutual authentication with key agreement scheme for mobile devices on elliptic curve cryptosystem. J Syst Softw 84(11):1892–1898, DOI 10.1016/j.jss.2011.06.061
45. Hung-Min Sun, Muh-Chyi Leu (2009) An Efficient Authentication Scheme for Access Control in Mobile Pay-TV Systems. IEEE Trans Multimed 11(5):947–959, DOI 10.1109/TMM.2009.2021790
46. Yang X, Huang X, Liu JK (2016) Efficient handover authentication with user anonymity and untraceability for Mobile Cloud Computing. Futur Gener Comput Syst 62:190–195, DOI 10.1016/j.future.2015.09.028
47. Liu J, Zhang Z, Chen X, Kwak KS (2014) Certificateless Remote Anonymous Authentication Schemes for WirelessBody Area Networks. IEEE Trans Parallel Distrib Syst 25(2):332–342, DOI 10.1109/TPDS.2013.145
48. Guo L, Zhang C, Sun J, Fang Y (2014) A Privacy-Preserving Attribute-Based Authentication System for Mobile Health Networks. IEEE Trans Mob Comput 13(9):1927–1941, DOI 10.1109/TMC.2013.84
49. Sun J, Zhang R, Zhang J, Zhang Y (2014) TouchIn: Sightless two-factor authentication on multi-touch mobile devices. In: 2014 IEEE Conf. Commun. Netw. Secur., IEEE, pp 436–444, DOI 10.1109/CNS.2014.6997513
50. Wu TY, Tseng YM (2010) An efficient user authentication and key exchange protocol for mobile clientâĂŞserver environment. Comput Networks 54(9):1520–1530, DOI 10.1016/j.comnet.2009.12.008
51. Chien-Ming Chen, King-Hang Wang, Tsu-Yang Wu, Jeng-Shyang Pan, Hung-Min Sun (2013) A Scalable Transitive Human-Verifiable Authentication Protocol for Mobile Devices. IEEE Trans Inf Forensics Secur 8(8):1318–1330, DOI 10.1109/TIFS.2013.2270106
52. Jeong YS, Park JS, Park JH (2015) An efficient authentication system of smart device using multi factors in mobile cloud service architecture. Int J Commun Syst 28(4):659–674, DOI 10.1002/dac.2694
53. Clarke N, Furnell S (2007) Advanced user authentication for mobile devices. Comput Secur 26(2):109–119, DOI 10.1016/j.cose.2006.08.008
54. Clarke NL, Furnell SM (2006) Authenticating mobile phone users using keystroke analysis. Int J Inf Secur 6(1):1–14, DOI 10.1007/s10207-006-0006-6
55. Crawford H, Renaud K, Storer T (2013) A framework for continuous, transparent mobile device authentication. Comput Secur 39:127–136, DOI 10.1016/j.cose.2013.05.005
56. Abate AF, Nappi M, Ricciardi S (2017) I-Am: Implicitly Authenticate Me Person Authentication on Mobile Devices Through Ear Shape and Arm Gesture. IEEE Trans Syst Man, Cybern Syst pp 1–13, DOI 10.1109/TSMC.2017.2698258
57. Arteaga-Falconi JS, Al Osman H, El Saddik A (2016) ECG Authentication for Mobile Devices. IEEE Trans Instrum Meas 65(3):591–600, DOI 10.1109/TIM.2015.2503863
58. Kang SJ, Lee SY, Cho HI, Park H (2016) ECG Authentication System Design Based on Signal Analysis in Mobile and Wearable Devices. IEEE Signal Process Lett 23(6):805–808, DOI 10.1109/LSP.2016.2531996
59. Holz C, Buthpitiya S, Knaust M (2015) Bodyprint: Biometric user identification on mobile devices using the capacitive touchscreen to scan body part. In: Proc. 33rd Annu. ACM Conf. Hum. Factors Comput. Syst. - CHI '15, ACM Press, New York, New York, USA, pp 3011–3014, DOI 10.1145/2702123.2702518
60. Saevanee H, Clarke N, Furnell S, Biscione V (2015) Continuous user authentication using multi-modal biometrics. Comput Secur 53:234–246, DOI 10.1016/j.cose.2015.06.001
61. Hoang T, Choi D, Nguyen T (2015) Gait authentication on mobile phone using biometric cryptosystem and fuzzy commitment scheme. Int J Inf Secur 14(6):549–560, DOI 10.1007/s10207-015-0273-1

62. Chen Y, Sun J, Zhang R, Zhang Y (2015) Your song your way: Rhythm-based two-factor authentication for multi-touch mobile devices. In: 2015 IEEE Conf. Comput. Commun., IEEE, pp 2686–2694, DOI 10.1109/INFOCOM.2015.7218660
63. Seto J, Wang Y, Lin X (2015) User-Habit-Oriented Authentication Model: Toward Secure, User-Friendly Authentication for Mobile Devices. IEEE Trans Emerg Top Comput 3(1):107–118, DOI 10.1109/TETC.2014.2379991
64. Meng Y, Wong DS, Schlegel R, Kwok Lf (2013) Touch Gestures Based Biometric Authentication Scheme for Touchscreen Mobile Phones. In: Int. Conf. Inf. Secur. Cryptol., Springer, Berlin, Heidelberg, pp 331–350, DOI 10.1007/978-3-642-38519-3_21
65. Sae-Bae N, Ahmed K, Isbister K, Memon N (2012) Biometric-rich gestures. In: Proc. 2012 ACM Annu. Conf. Hum. Factors Comput. Syst. - CHI '12, ACM Press, New York, New York, USA, p 977, DOI 10.1145/2207676.2208543
66. Feng T, Liu Z, Kwon KA, Shi W, Carbunar B, Jiang Y, Nguyen N (2012) Continuous mobile authentication using touchscreen gestures. In: 2012 IEEE Conf. Technol. Homel. Secur., IEEE, pp 451–456, DOI 10.1109/THS.2012.6459891
67. Maiorana E, Campisi P, González-Carballo N, Neri A (2011) Keystroke dynamics authentication for mobile phones. In: Proc. 2011 ACM Symp. Appl. Comput. - SAC '11, ACM Press, New York, New York, USA, p 21, DOI 10.1145/1982185.1982190
68. Chang TY, Tsai CJ, Lin JH (2012) A graphical-based password keystroke dynamic authentication system for touch screen handheld mobile devices. J Syst Softw 85(5):1157–1165, DOI 10.1016/j.jss.2011.12.044
69. Tasia CJ, Chang TY, Cheng PC, Lin JH (2014) Two novel biometric features in keystroke dynamics authentication systems for touch screen devices. Secur Commun Networks 7(4):750–758, DOI 10.1002/sec.776
70. Kambourakis G, Damopoulos D, Papamartzivanos D, Pavlidakis E (2016) Introducing touchstroke: keystroke-based authentication system for smartphones. Secur Commun Networks 9(6):542–554, DOI 10.1002/sec.1061
71. Kim DS, Hong KS (2008) Multimodal biometric authentication using teeth image and voice in mobile environment. IEEE Trans Consum Electron 54(4):1790–1797, DOI 10.1109/TCE.2008.4711236
72. Frank M, Biedert R, Ma E, Martinovic I, Song D (2013) Touchalytics: On the Applicability of Touchscreen Input as a Behavioral Biometric for Continuous Authentication. IEEE Trans Inf Forensics Secur 8(1):136–148, DOI 10.1109/TIFS.2012.2225048
73. Mahbub U, Patel VM, Chandra D, Barbello B, Chellappa R (2016) Partial face detection for continuous authentication. In: 2016 IEEE Int. Conf. Image Process., IEEE, pp 2991–2995, DOI 10.1109/ICIP.2016.7532908
74. Sharaf-Dabbagh Y, Saad W (2016) On the authentication of devices in the Internet of things. In: 2016 IEEE 17th Int. Symp. A World Wireless, Mob. Multimed. Networks, IEEE, pp 1–3, DOI 10.1109/WoWMoM.2016.7523532
75. Richard Yu F, Tang H, Leung VCM, Liu J, Lung CH (2008) Biometric-based user authentication in mobilead hoc networks. Secur Commun Networks 1(1):5–16, DOI 10.1002/sec.6
76. He D (2012) An efficient remote user authentication and key agreement protocol for mobile clientâĂŞserver environment from pairings. Ad Hoc Networks 10(6):1009–1016, DOI 10.1016/j.adhoc.2012.01.002
77. He D, Kumar N, Shen H, Lee JH (2016) One-to-many authentication for access control in mobile pay-TV systems. Sci China Inf Sci 59(5):052108, DOI 10.1007/s11432-015-5469-5
78. Islam SH, Khan MK (2016) Provably secure and pairing-free identity-based handover authentication protocol for wireless mobile networks. Int J Commun Syst 29(17):2442–2456, DOI 10.1002/dac.2847
79. Wu L, Zhang Y, Xie Y, Alelaiw A, Shen J (2017) An Efficient and Secure Identity-Based Authentication and Key Agreement Protocol with User Anonymity for Mobile Devices. Wirel Pers Commun 94(4):3371–3387, DOI 10.1007/s11277-016-3781-z
80. Almuairfi S, Veeraraghavan P, Chilamkurti N (2013) A novel image-based implicit password authentication system (IPAS) for mobile and non-mobile devices. Math Comput Model 58(1-2):108–116, DOI 10.1016/j.mcm.2012.07.005
81. Shi L, Li M, Yu S, Yuan J (2013) BANA: Body Area Network Authentication Exploiting Channel Characteristics. IEEE J Sel Areas Commun 31(9):1803–1816, DOI 10.1109/JSAC.2013.130913
82. De Marsico M, Galdi C, Nappi M, Riccio D (2014) FIRME: Face and Iris Recognition for Mobile Engagement. Image Vis Comput 32(12):1161–1172, DOI 10.1016/j.imavis.2013.12.014
83. Shahandashti SF, Safavi-Naini R, Safa NA (2015) Reconciling user privacy and implicit authentication for mobile devices. Comput Secur 53:215–233, DOI 10.1016/j.cose.2015.05.009
84. Khamis M, Alt F, Hassib M, von Zezschwitz E, Hasholzner R, Bulling A (2016) GazeTouchPass. In: Proc. 2016 CHI Conf. Ext. Abstr. Hum. Factors Comput. Syst. - CHI EA '16, ACM Press, New York, New

York, USA, pp 2156–2164, DOI 10.1145/2851581.2892314
85. Shahzad M, Liu AX, Samuel A (2017) Behavior Based Human Authentication on Touch Screen Devices Using Gestures and Signatures. IEEE Trans Mob Comput 16(10):2726–2741, DOI 10.1109/TMC.2016.2635643
86. Hankerson D, Menezes AJ, Vanstone S (2006) Guide to elliptic curve cryptography. Springer Science & Business Media
87. Ferrag MA, Maglaras L, Argyriou A, Kosmanos D, Janicke H (2018) Security for 4G and 5G cellular networks: A survey of existing authentication and privacy-preserving schemes. J Netw Comput Appl 101:55–82, DOI 10.1016/j.jnca.2017.10.017
88. Ferrag MA, Maglaras LA, Janicke H, Jiang J, Shu L (2018) A systematic review of data protection and privacy preservation schemes for smart grid communications. Sustainable Cities and Society 38:806–835
89. Wang D, He D, Wang P, Chu CH (2014) Anonymous two-factor authentication in distributed systems: Certain goals are beyond attainment. IEEE Transactions on Dependable and Secure Computing 12(4):428–442
90. Li X, Niu J, Kumari S, Wu F, Choo KKR (2018) A robust biometrics based three-factor authentication scheme for Global Mobility Networks in smart city. Futur Gener Comput Syst 83:607–618, DOI 10.1016/j.future.2017.04.012
91. Li W, Gu Q, Zhao Y, Wang P (2017) Breaking Two Remote User Authentication Systems for Mobile Devices. In: 2017 IEEE 3rd Int. Conf. Big Data Secur. Cloud (BigDataSecurity), IEEE Int. Conf. High Perform. Smart Comput. IEEE Int. Conf. Intell. Data Secur., IEEE, pp 37–42, DOI 10.1109/BigDataSecurity.2017.34
92. Jia Z, Zhang Y, Shao H, Lin Y, Wang J (2006) A Remote User Authentication Scheme Using Bilinear Pairings and ECC. In: Sixth Int. Conf. Intell. Syst. Des. Appl., IEEE, vol 2, pp 1091–1094, DOI 10.1109/ISDA.2006.253764
93. Wang D, Li W, Wang P (2018) Measuring two-factor authentication schemes for real-time data access in industrial wireless sensor networks. IEEE Transactions on Industrial Informatics 14(9):4081–4092
94. Wang D, Wang P (2016) Two birds with one stone: Two-factor authentication with security beyond conventional bound. IEEE transactions on dependable and secure computing 15(4):708–722
95. Wang D, Gu Q, Cheng H, Wang P (2016) The request for better measurement: A comparative evaluation of two-factor authentication schemes. In: Proceedings of the 11th ACM on Asia Conference on Computer and Communications Security, ACM, pp 475–486
96. Zhang Q, Li H, Sun Z, Tan T (2018) Deep feature fusion for iris and periocular biometrics on mobile devices. IEEE Transactions on Information Forensics and Security 13(11):2897–2912
97. Samangouei P, Patel VM, Chellappa R (2017) Facial attributes for active authentication on mobile devices. Image Vis Comput 58:181–192, DOI 10.1016/j.imavis.2016.05.004
98. Wu L, Wang J, Choo KKR, He D (2018) Secure key agreement and key protection for mobile device user authentication. IEEE Transactions on Information Forensics and Security 14(2):319–330
99. Sitova Z, Sedenka J, Yang Q, Peng G, Zhou G, Gasti P, Balagani KS (2016) HMOG: New Behavioral Biometric Features for Continuous Authentication of Smartphone Users. IEEE Trans Inf Forensics Secur 11(5):877–892, DOI 10.1109/TIFS.2015.2506542
100. Fridman L, Weber S, Greenstadt R, Kam M (2017) Active Authentication on Mobile Devices via Stylometry, Application Usage, Web Browsing, and GPS Location. IEEE Syst J 11(2):513–521, DOI 10.1109/JSYST.2015.2472579
101. Boechat GC, Ferreira JC, Carvalho Filho ECB (2007) Authentication personal. In: 2007 Int. Conf. Intell. Adv. Syst., IEEE, pp 254–256, DOI 10.1109/ICIAS.2007.4658385
102. Gragnaniello D, Sansone C, Verdoliva L (2015) Iris liveness detection for mobile devices based on local descriptors. Pattern Recognit Lett 57:81–87, DOI 10.1016/j.patrec.2014.10.018
103. Feng Q, He D, Zeadally S, Kumar N, Liang K (2018) Ideal lattice-based anonymous authentication protocol for mobile devices. IEEE Systems Journal (99):1–11
104. McKeown N, Anderson T, Balakrishnan H, Parulkar G, Peterson L, Rexford J, Shenker S, Turner J (2008) Openflow: enabling innovation in campus networks. ACM SIGCOMM Computer Communication Review 38(2):69–74
105. Doria A, Salim JH, Haas R, Khosravi H, Wang W, Dong L, Gopal R, Halpern J (2010) Forwarding and control element separation (forces) protocol specification. Tech. rep.
106. Wang D, Cheng H, He D, Wang P (2016) On the challenges in designing identity-based privacy-preserving authentication schemes for mobile devices. IEEE Systems Journal 12(1):916–925
107. Truong TT, Tran MT, Duong AD (2012) Improvement of the more efficient and secure id-based remote mutual authentication with key agreement scheme for mobile devices on ecc. In: 2012 26th International Conference on Advanced Information Networking and Applications Workshops, IEEE, pp 698–703

108. Li X, Zhang Y, Liu X, Cao J, Zhao Q (2012) A lightweight roaming authentication protocol for anonymous wireless communication. In: 2012 IEEE Global Communications Conference (GLOBECOM), IEEE, pp 1029–1034
109. Zhang G, Fan D, Zhang Y, Li X, Liu X (2015) A privacy preserving authentication scheme for roaming services in global mobility networks. Security and Communication Networks 8(16):2850–2859
110. Wang Z (2017) An identity-based data aggregation protocol for the smart grid. IEEE Transactions on Industrial Informatics 13(5):2428–2435
111. Wang Z (2018) A privacy-preserving and accountable authentication protocol for iot end-devices with weaker identity. Future Generation Computer Systems 82:342–348
112. Chen CL (2008) A secure and traceable E-DRM system based on mobile device. Expert Syst Appl 35(3):878–886, DOI 10.1016/j.eswa.2007.07.029
113. (2016) Android malware defeats two-factor authentication. https://www.welivesecurity.com/2016/03/09/android-trojan-targets-online-banking-users/, accessed: 2018-03-11
114. (2016) Android banking trojan masquerades as flash player and bypasses 2fa. https://thestack.com/security/2016/01/18/android-malware-defeats-two-factor-authentication/, accessed: 2018-03-11
115. (2018) Unhackable computer under development with 3.6m darpa grant. http://ns.umich.edu/new/releases/25336-unhackable-computer-under-development-with-3-6 accessed: 2018-03-11
116. Maglaras LA, Jiang J (2014) Ocsvm model combined with k-means recursive clustering for intrusion detection in scada systems. In: Heterogeneous Networking for Quality, Reliability, Security and Robustness (QShine), 2014 10th International Conference on, IEEE, pp 133–134
117. Dewa Z, Maglaras LA (2016) Data mining and intrusion detection systems. International Journal of Advanced Computer Science and Applications 7(1):62–71
118. Li B, Lu R, Wang W, Choo KKR (2017) Distributed host-based collaborative detection for false data injection attacks in smart grid cyber-physical system. Journal of Parallel and Distributed Computing 103:32–41
119. Nguyen VG, Brunstrom A, Grinnemo KJ, Taheri J (2017) Sdn/nfv-based mobile packet core network architectures: a survey. IEEE Communications Surveys & Tutorials 19(3):1567–1602
120. Maglaras L, Ferrag MA, Derhab A, Mukherjee M, Janicke H (2019) Cyber security: From regulations and policies to practice. In: Strategic Innovative Marketing and Tourism, Springer, pp 763–770
121. Harrison S, Tzounis A, Maglaras LA, Siewe F, Smith R, Janicke H (2016) A security evaluation framework for uk e-goverment services agile software development. arXiv preprint arXiv:160402368